

**BEFORE THE
UNITED STATES JUDICIAL PANEL ON
MULTIDISTRICT LITIGATION**

**IN RE: KEFFER DEVELOPMENT
SERVICES, LLC LITIGATION**

MDL DOCKET NO. _____

**KEFFER DEVELOPMENT SERVICES, LLC MOTION TO TRANSFER RELATED
CASES FOR CONSOLIDATED PRETRIAL PROCEEDINGS
PURSUANT TO 28 U.S.C. 4 1407**

**DILLON, MCCANDLESS, KING,
COULTER & GRAHAM LLP**

Thomas W. King, III
PA I.D. No. 21580
tking@dmkcg.com

Jordan P. Shuber
PA I.D. No. 317823
jshuber@dmkcg.com

Carl A. Fejko
PA I.D. No. 331216
cfejko@dmkcg.com

Kyle S. Uhlman
CA I.D. No. 302292
kuhlman@dmkcg.com

128 West Cunningham Street
Butler, PA 16001
Telephone: 724-283-2200
Facsimile: 724-283-2298

**BEFORE THE
UNITED STATES JUDICIAL PANEL ON
MULTIDISTRICT LITIGATION**

**IN RE: KEFFER DEVELOPMENT
SERVICES, LLC LITIGATION**

MDL DOCKET NO. _____

**KEFFER DEVELOPMENT SERVICES, LLC MOTION TO TRANSFER RELATED
CASES FOR CONSOLIDATED PRETRIAL PROCEEDINGS
PURSUANT TO 28 U.S.C. 4 1407**

Keffer Development Services, LLC (“Keffer”) is a Defendant in eight cases in the U.S. District Court for the Eastern District of Michigan and five other cases pending in federal courts throughout the country. Keffer hereby moves for an Order for transfer and consolidation pursuant to 28 U.S.C. § 1407 for the civil actions listed in the Schedule of Actions filed concurrently herewith.

For the reasons set forth herein and in Keffer’s accompanying Brief in Support, Keffer respectfully requests that the Panel issue an Order transferring the thirteen actions listed in the accompanying Schedule of Actions, as well as all subsequently filed related actions, to the U.S. District Court for the Eastern District of Michigan for coordinated or consolidated pretrial proceedings.

Dated: June 5, 2025

Respectfully submitted,

**DILLON, MCCANDLESS, KING,
COULTER & GRAHAM LLP**

By: /s/ Thomas W. King, III

Thomas W. King, III

PA I.D. No. 21580

tking@dmkcg.com

Jordan P. Shuber

PA I.D. No. 317823

jshuber@dmkcg.com

Carl A. Fejko

PA I.D. No. 331216

cfejko@dmkcg.com

Kyle S. Uhlman

CA I.D. No. 302292

kuhlman@dmkcg.com

128 West Cunningham Street

Butler, PA 16001

Telephone: 724-283-2200

Facsimile: 724-283-2298

TKing@dmkcg.com

*Attorneys for Defendant Keffer
Development Services, LLC*

**BEFORE THE
UNITED STATES JUDICIAL PANEL ON
MULTIDISTRICT LITIGATION**

**IN RE: KEFFER DEVELOPMENT
SERVICES, LLC LITIGATION**

MDL DOCKET NO. _____

**BRIEF IN SUPPORT OF KEFFER DEVELOPMENT SERVICES, LLC MOTION
TO TRANSFER RELATED CASES FOR CONSOLIDATED
PRETRIAL PROCEEDINGS PURSUANT TO 28 U.S.C. § 1407**

**DILLON, MCCANDLESS, KING,
COULTER & GRAHAM LLP**

Thomas W. King, III
PA I.D. No. 21580
tking@dmkcg.com

Jordan P. Shuber
PA I.D. No. 317823
jshuber@dmkcg.com

Carl A. Fejko
PA I.D. No. 331216
cfejko@dmkcg.com

Kyle S. Uhlman
CA I.D. No. 302292
kuhlman@dmkcg.com

128 West Cunningham Street
Butler, PA 16001
Telephone: 724-283-2200
Facsimile: 724-283-2298

**BEFORE THE
UNITED STATES JUDICIAL PANEL ON
MULTIDISTRICT LITIGATION**

**IN RE: KEFFER DEVELOPMENT
SERVICES, LLC LITIGATION**

MDL DOCKET NO. _____

**BRIEF IN SUPPORT OF KEFFER DEVELOPMENT SERVICES, LLC MOTION TO TRANSFER
RELATED CASES FOR CONSOLIDATED
PRETRIAL PROCEEDINGS PURSUANT TO 28 U.S.C. § 1407**

INTRODUCTION

Keffer Development Services, LLC (“Keffer”) is a defendant in thirteen identical cases pending in federal courts across the United States—twelve of which are putative class actions. Eight cases are currently pending in the U.S. District Court for the Eastern District of Michigan, with the remaining five filed in federal courts in various other jurisdictions. Similar Plaintiffs’ firms nationwide appear to be actively filing or preparing to file additional related actions, nationwide.

As the volume of federal litigation increases, so do the burdens of managing duplicative discovery, conflicting rulings, and procedural inefficiencies. Accordingly, Keffer seeks an order pursuant to 28 U.S.C. § 1407 and JPML Rule 6.2 consolidating the thirteen currently filed cases—listed in the accompanying Schedule of Actions—and any subsequently filed tag-along actions, in the U.S. District Court for the Eastern District of Michigan.

BACKGROUND

Keffer Development Services, LLC (“Keffer”), a Pennsylvania-based limited liability company, is a common defendant in a series of federal lawsuits arising from allegations that

former University of Michigan¹ football coach Matthew Weiss exploited vulnerabilities in student-athlete data systems employed and utilized by Keffer in various universities throughout the country. These lawsuits, all filed since March of this year, and now occurring across six jurisdictions, accuse Weiss of accessing sensitive personal information of over 150,000 athletes across more than 100 institutions between 2015 and January 2023. The plaintiffs allege that Weiss used this information to hack into the social media, email, and cloud storage accounts of at least 3,300 individuals, predominantly female student-athletes, to obtain intimate photos and videos without their consent.

The lawsuits all assert that Keffer provided electronic medical record and student-athlete training systems, via Athletic Trainer System software, to numerous universities, failed to implement adequate security measures to protect the data it managed. The various plaintiffs around the country have alleged that this negligence facilitated Weiss's unauthorized access to the sensitive information stated above. The claims against Keffer include violations under the Computer Fraud and Abuse Act, the Stored Communications Act, Title IX, and various state laws, encompassing allegations of invasion of privacy, gross negligence, and intentional infliction of emotional distress.

Keffer has denied wrongdoing and intends to vigorously defend itself against the allegations. The company maintains that it fully cooperated with law enforcement during the investigation and disputes the claims of negligence and misconduct.

This proposed multidistrict litigation consolidates numerous lawsuits filed across various federal courts, including the Eastern District of Michigan, the Middle District of North

¹ Notably, eight cases were consolidated in the Eastern District of Michigan, where Keffer seeks to formulate this MDL.

Carolina, the Northern District of Ohio, the Central District of California, the Northern District of Illinois, and the District of Massachusetts. The cases involve multiple universities, including the University of Michigan, High Point University, Malone University, Loyola University Chicago, and Simmons University, all of which are alleged to have failed to adequately protect student-athlete data, thereby enabling Weiss's alleged misconduct.

The central issue in this litigation is whether Keffer and the implicated universities exercised reasonable care in safeguarding sensitive student data and whether their actions or inactions contributed to the alleged breaches of privacy and subsequent harm to the plaintiffs. Thirteen lawsuits against Keffer are currently pending in six federal districts as follows, and as set out in the attached Schedule of Actions (the "Actions"):

a. Eastern District of Michigan:

i. JANE DOE 1, and JANE DOE 2 vs. MATTHEW WEISS; the REGENTS OF THE UNIVERSITY OF MICHIGAN; the UNIVERSITY OF MICHIGAN; KEFFER DEVELOPMENT SERVICES, LLC, No. 2:25-cv-10806 (E.D. MI) (March 21, 2025)

ii. JANE DOE 1, and JANE DOE 2, obo themselves and others similarly situated, vs. MATTHEW WEISS; the REGENTS OF THE UNIVERSITY OF MICHIGAN; the UNIVERSITY OF MICHIGAN; KEFFER DEVELOPMENT SERVICES, LLC, No. 2:25-cv-10855 (E.D. MI) (March 26, 2025)

iii. JANE DOE 1 vs. MATTHEW WEISS; the REGENTS OF THE UNIVERSITY OF MICHIGAN; the UNIVERSITY OF MICHIGAN; KEFFER DEVELOPMENT SERVICES, LLC, No. 2:25-cv-10988 (E.D. MI) (April 7, 2025)

iv. JANE DOE 1, obo herself and others similarly situated, vs. THE UNIVERSITY OF MICHIGAN BOARD OF REGENTS; KEFFER DEVELOPMENT SERVICES, LLC, and MATTHEW WEISS, No. 2:25-cv-10951 (E.D. MI) (April 2, 2025)

v. JANE DOE 1, obo herself and others similarly situated, vs. THE UNIVERSITY OF MICHIGAN BOARD OF REGENTS; KEFFER DEVELOPMENT SERVICES, LLC, and MATTHEW WEISS, No. 2:25-cv-10876 (E.D. MI) (March 28, 2025)

vi. STUDENT DOE 1, obo herself and others similarly situated, vs. THE UNIVERSITY OF MICHIGAN BOARD OF REGENTS; KEFFER DEVELOPMENT SERVICES, LLC, and MATTHEW WEISS, No. 2:25-cv-10999 (E.D. MI) (April 8, 2025)

vii. JANE DOE 1, JANE DOE 2, JANE DOE 3, JANE DOE 4, JANE DOE 5, JANE DOE 6, JANE DOE 7, JANE DOE 8, JANE DOE 9, JANE DOE 10, and JANE DOE 11, vs. THE REGENTS OF THE UNIVERSITY OF MICHIGAN; the UNIVERSITY OF MICHIGAN; KEFFER DEVELOPMENT SERVICES, LLC, and MATTHEW WEISS, No. 2:25-cv-10946 (E.D. MI) (April 2, 2025)

viii. JANE ROE CLF 001 vs. MATTHEW WEISS; THE REGENTS OF THE UNIVERSITY OF MICHIGAN; THE UNIVERISTY OF MICHIGAN; KEFFER DEVELOPMENT SERVICES, LLC, No. 2:25-cv-10870 (E.D. MI) (March 27, 2025)

b. Northern District of Illinois: JANE DOE 1 vs. MATTHEW WEISS; LOYALA UNIVERSITY CHICAGO, AND KEFFER DEVELOPMENT SERVICES, LLC, No. 2:25-cv-04233 (N.D. IL) (April 17, 2025)

c. Northern District of Ohio: JANE DOE 1 vs. MATTHEW WEISS, MALONE UNIVERSITY and KEFFER DEVELOPMENT, LLC, No. 5:25-cv-00827 (N.D. OH) (April 24, 2025)

d. Central District of California: JANE DOE 1 vs. MATTHEW WEISS, CALIFORNIA STATE UNIVERSITY, SAN BERNARDINO, BOARD OF TRUSTEES OF THE CALIFORNIA STATE UNIVERSITY, and KEFFER DEVELOPMENT SERVICES, LCC, No. 5:25-cv-00997 (C.D. CA) (April 23, 2025)

e. Middle District of North Carolina: JANE DOES 1 and 2 vs. MATTHEW WEISS, HIGH POINT UNIVERSITY, and KEFFER DEVELOPMENT SERVICES, LLC, No. 1:25-cv-00303 (M.D. NC) (April 23, 2025)

f. District Court of Massachusetts: JANE DOE vs. MATTHEW WEISS; the TRUSTEES OF SIMMONS UNIVERSITY; SIMMONS UNIVERSITY; and KEFFER DEVELOPMENT SERVICES, LLC, No. 1:25-cv-11151, (D.C. MA) (April 28, 2025)

LEGAL STANDARD

Transfer and consolidation of federal cases is appropriate when actions pending in different judicial districts involve similar questions of fact such that consolidating pretrial

proceedings would “promote the just and efficient conduct of such actions.” 28 U.S.C. § 1407.

In relevant part, Section 1407 provides:

When civil actions involving one or more common questions of fact are pending in different districts, such actions may be transferred to any district for coordinated or consolidated pretrial proceedings. Such transfers shall be made by the judicial panel on multidistrict litigation authorized by this section upon its determination that transfers for such proceedings will be for the convenience of parties and witnesses and will promote the just and efficient conduct of such actions.

All of these suits directly overlap in many ways. Twelve are class actions brought on behalf of nationwide classes and/or subclasses based on plaintiff age or state of residency. All of the complaints name Keffer as a defendant, and all actions also name Matthew Weiss and an educational institution.

ARGUMENT

The transfer and coordination of the Actions is appropriate and necessary in the case at hand.

Multidistrict litigation is designed “to promote the just and efficient conduct’ of ‘civil actions involving one or more common questions of fact’ that are pending in different districts.” *In re Phenylpropanolamine (PPA) Prods. Liab. Litig.*, 460 F.3d 1217, 1229 (9th Cir. 2006) (quoting 28 U.S.C. § 1407(a)). Transfer is appropriate where it will serve “the convenience of parties and witnesses and will promote the just and efficient conduct of such actions.” 28 U.S.C. § 1407.

Upon receiving a motion to transfer, the Panel “analyzes each group of cases in light of the statutory criteria and the primary purposes of the MDL process to determine whether transfer is appropriate.” *In re PPA Prods. Liab. Litig.*, 460 F.3d at 1230. Four factors help determine whether transfer will facilitate the convenience of the parties and promote the just and efficient conduct of the transferred case: (1) elimination of duplicative discovery; (2) avoidance of conflicting rulings and schedules; (3) reduction of litigation costs; and (4) conservation of the time and effort of the

parties, attorneys, witnesses, and courts. Manual for Complex Litigation (Fourth), § 20.131, at 219. To that end, centralization is appropriate to eliminate duplicative discovery, prevent inconsistent rulings, and conserve the resources of the parties, their counsel, and the judiciary. *See, e.g., In re Proven Networks, LLC, Pat. Litig.*, 492 F. Supp. 3d 1338, 1340 (J.P.M.L. 2020) (noting those factors in ordering consolidation).

Transfer is appropriate here because the Actions share common issues of fact and law and are in the early stages of litigation. To Plaintiffs' knowledge, Initial Case Management Conferences have yet to occur in any of the cases listed in the Schedule of Actions filed herewith. Further, there are motions filed in numerous cases, and stipulations to extend deadlines, including briefing schedules for proposed motions, that have been entered. Accordingly, consolidated proceedings will streamline discovery, avoid inconsistent pretrial rulings, and preserve judicial and party resources.

The Actions share common questions of fact and law that merit transfer and consolidation.

The threshold requirement of Section 1407 is that there be questions of fact and law common to the cases for which MDL treatment is sought. Commonalities in factual and legal questions need not be complete, nor even the majority, to merit transfer. *In re Katz Interactive Call Processing Pat. Litig.*, 481 F. Supp. 2d 1353, 1355 (J.P.M.L. 2007). “[I]ndividualized factual issues” do not “negate the efficiencies to be gained by centralization.” *In re Nat’l Prescription Opiate Litig.*, 290 F. Supp. 3d 1375, 1379 (J.P.M.L. 2017).

The Actions here share sufficient common factual and legal questions. The claims in each of those actions arise from the same course of conduct by the defendants. Among the numerous common questions of fact are:

- What specific data systems did Keffer provide to the universities, and what types of data did these systems store?
- What cybersecurity protocols and safeguards did Keffer implement to protect student-athlete information?
- Did Keffer comply with industry standards or legal obligations (e.g., FERPA, HIPAA where applicable, or other privacy laws)?
- Was there a known vulnerability or deficiency in Keffer's software that could have been exploited?
- How did Matthew Weiss allegedly access the sensitive data?
- Did the data breaches result from a vulnerability in Keffer's software or a failure in its security policies?
- Was Keffer aware—or should it have been aware—of any prior incidents or potential breaches?
- Did Keffer knowingly or negligently permit access to third parties like Weiss?
- Did Keffer have any professional or contractual relationship with Matthew Weiss?
- To what extent did Keffer's actions (or inactions) contribute to Weiss's ability to obtain sensitive information?
- Did Keffer owe a duty of care to the student-athletes whose data it managed, even though they were not direct clients?
- Did Keffer breach that duty through inadequate data security or oversight?
- Were there warnings, red flags, or complaints that Keffer failed to act on before the breach occurred?

- What information did Keffer provide to universities about system vulnerabilities or security features?
- Were universities adequately informed about how to configure and maintain secure environments with Keffer's products?
- Did Keffer perform any audits, security checks, or provide updates to mitigate risks?
- Was the sensitive data actually accessed, and if so, how many individuals were affected across institutions?
- Was the breach preventable, and did Keffer's security failures cause or contribute to emotional, reputational, or economic harm?
- Did Keffer have a plan for incident response and mitigation?

Given that these common issues exist in each related case, in some form or another, MDL treatment is appropriate.

Transfer will serve the convenience of the parties and witnesses and promote the just and efficient conduct of the Actions.

Transfer and consolidation of similar actions is appropriate when it would enhance the convenience of the litigation and promote the just and efficient conduct of the actions to be coordinated. Here, pretrial coordination of the Actions will ease the burdens on the parties and the judicial system. All of the Actions are in their early stages and to alleviate the parties' burden, stipulations to adjust briefing schedules for these motions will be requested as more and more cases are being filed. To the best of the undersigned's knowledge, no discovery has occurred in any of the Actions. The first action was filed in the Eastern District of Michigan, only several hours from where Keffer maintains its principal place of business, approximately two months ago. Now is the optimal time for coordination, for the convenience of the parties and witnesses and to ensure a just and

efficient resolution of the Actions and similar cases yet to be filed. Consolidation by this Panel will avoid the waste of duplicative discovery and the risk of inconsistent rulings and will result in conservation of judicial and party resources. Taken collectively, these factors establish that the Actions are appropriate for coordination under 28 U.S.C. § 1407.

Pretrial transfer will reduce the burden and costs of discovery significantly for both the parties to the Actions and the judiciary. The pending actions share the same basic theory of liability and underlying factual allegations and injuries, such that all cases will involve the same core discovery, fact witnesses, and general liability and causation experts. MDL treatment will enable a single court to establish a pretrial plan that will minimize the inconvenience and expenses of duplicative discovery, which is precisely the purpose of transfer and coordination under Section 1407.

Consolidation will also permit both Plaintiffs' and Defendants' counsel to coordinate efforts and share the pretrial workload among the various and numerous counsel working on this matter. Instead of different law firms pursuing different litigation strategies and engaging in duplicative discovery and motion practice, a coordinated team of attorneys can pursue the claims in one court, before one judge, preserving both Plaintiffs' and Defendants' resources and allowing their attorneys to work together in common to further these cases. The Panel has previously endorsed this rationale, noting that "prudent counsel will combine their forces and apportion the workload in order to streamline the efforts of the parties and witnesses, their counsel and the judiciary, thereby effectuating an overall savings of case and a minimum of inconvenience to all concerned." *In re Baldwin-United Corp. Litig.*, 581 F. Supp. 739, 741 (J.P.M.L. 1984).

Additionally, pretrial centralization will enable Defendants to concentrate their attention and discovery efforts in one federal forum, rather than numerous district courts throughout the country. As a result, Defendants will be able to move quickly and effectively through discovery, enhancing

the overall efficiency of the litigation. *See In re Apple iPhone 3G Prod. Liab. Litig.*, 630 F. Supp. 2d 1382, 1383 (J.P.M.L. 2009) (noting efficiency obtained through MDL process). Rather than conducting general discovery in thirteen different actions in at least six different district courts, written discovery and depositions of key witnesses can be coordinated and completed just once. This ability to streamline the work of discovery and coordinate efforts among counsel will serve the interests of justice.

Further, discovery has yet to begin in the Michigan Eastern District and there are currently no discovery orders, bellwether selection process, or trials set. Therefore, it would be impeccable timing for establishing an MDL now, as the opportunity remains to comprehensively coordinate discovery.

A single centralized and coordinated pretrial plan will also further fairness and efficiency by avoiding inconsistent pretrial rulings. *See In re Levaquin Prods. Liab. Litig.*, 560 F. Supp. 2d 1384, 1385 (J.P.M.L. 2008). There are already thirteen related cases pending in six district courts involving multiple different Plaintiffs' counsel, with many more to come. As discussed above, numerous identical motions have been filed (or are anticipated to be filed), including several pending before different judges in the same district court. Inconsistent rulings are inevitable as these various courts set discovery and trial schedules and tackle individual motions. Transfer and consolidation will avoid this serious risk.

MDL treatment will enable a single court to establish a pretrial plan that will minimize the inconvenience and expenses of litigating numerous cases separately, which is precisely the purpose of transfer and coordination under Section 1407. Transferring the Actions for pretrial coordination will make this litigation far more efficient and convenient for all involved. One court overseeing these actions will allow the judiciary to conserve limited resources. If transfer is denied, however, the Actions and tag-along cases will proceed on independent tracks in at least six different courts, requiring

duplicative discovery, including repeated depositions of the same corporate personnel and expert witnesses, risking inconsistent rulings and wasting resources.

The Eastern District of Michigan is the most suitable forum for this MDL.

Pursuant to 28 U.S.C. § 1407, the Judicial Panel on Multidistrict Litigation (JPML) is authorized to transfer civil actions involving common questions of fact to a single district “for coordinated or consolidated pretrial proceedings.” The key criteria for such consolidation include the convenience of parties and witnesses and the promotion of the just and efficient conduct of the litigation. In the present litigation involving Keffer Development Services, LLC and Matthew Weiss, the Eastern District of Michigan (“EDM”) is the most suitable and logical venue for centralization.

Under 28 U.S.C. § 1407(a):

When civil actions involving one or more common questions of fact are pending in different districts, such actions may be transferred to any district for coordinated or consolidated pretrial proceedings...for the convenience of parties and witnesses and will promote the just and efficient conduct of such actions.

Relevant factors considered by the JPML include:

- Location of witnesses and evidence;
- Judicial experience with similar cases;
- The nexus between the forum and the factual issues;
- The number and concentration of actions already pending in that district; and
- Resources and docket conditions of the district.

See: *In re Nat’l Prescription Opiate Litig.*, 290 F. Supp. 3d 1375 (J.P.M.L. 2017), *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 289 F. Supp. 3d 1322 (J.P.M.L. 2017)

The EDM has a factual nexus to the core allegations. Firstly, Matthew Weiss, as a former assistant football coach at the University of Michigan, allegedly accessed data from student-athletes nationwide by exploiting vulnerabilities in university systems and/or Keffer-related platforms. Secondly, the initial and most detailed investigations by law enforcement originated in Ann Arbor, Michigan, which lies within the Eastern District. Additionally, the University of Michigan is a named defendant in numerous lawsuits and is centrally involved in the factual matrix. All of these facts converge to show that the EDM represents the epicenter of the alleged wrongdoing, supporting centralization. See: *In re Michigan Flint Water Cases*, 192 F. Supp. 3d 1380, 1381 (J.P.M.L. 2016) (choosing E.D. Mich. because it was the “focal point of the events giving rise to this litigation”).

The EDM also has a concentration of related actions as a significant number of the pending cases—including the earliest-filed and most developed complaints—are already lodged in the EDM. Centralizing all the Actions in a district where litigation is already underway supports judicial economy and avoids duplication. See: *In re Epipen (Epinephrine Injection, USP) Mktg., Sales Practices & Antitrust Litig.*, 268 F. Supp. 3d 1353, 1355 (J.P.M.L. 2017) (“We generally select a transferee district where a number of actions are already pending.”).

The EDM also has the experience and resources to handle multidistrict litigation. In fact, the EDM has demonstrated an ability to manage large-scale MDLs and complex technical and privacy litigation, including high-profile data breach and product liability cases. The district also has judges experienced in managing multi-party, privacy-based, and technology-related litigation. Finally, docket conditions in the EDM are manageable compared to congested venues like the Northern District of Illinois or Central District of California. See: *In*

re Ford Motor Co. DPS6 Powershift Transmission Prods. Liab. Litig., 289 F. Supp. 3d 1350 (J.P.M.L. 2018).

The EDM provides convenience for the most parties and witnesses. Key parties, particularly Weiss and the University of Michigan, are located in or near the district, as well as likely witnesses, including Michigan-based university staff, data security personnel, and law enforcement agents involved in the original criminal investigation. The University of Michigan's IT systems, as part of the allegations, are also housed in the district. Keffer, though based in Pennsylvania, allegedly interacted with Michigan systems and personnel, making this district equally relevant to its defense, and Keffer's location in northwestern Pennsylvania means that—save for its home district—the EDM arguably provides the most convenience for them as well.

When looking at the other possible venues involved in this litigation, it is clear that the opposing venues are less suitable than the EDM. While other universities named as defendants are spread across the country, none hold as central a role in the alleged scheme as Michigan; and, as stated above, Keffer Development Services, though based in Pennsylvania, allegedly interacted with Michigan systems and personnel, making this district equally relevant to its defense. As such, consolidating elsewhere would likely result in duplicative discovery and inconvenience key witnesses and defendants most closely tied to the central events. For these reasons, the Eastern District of Michigan is the most appropriate forum for the centralized multidistrict litigation involving Keffer Development Services, LLC, Matthew Weiss, and associated universities. It is the factual, procedural, and logistical hub of the controversy, and consolidation there would best serve the interests of judicial efficiency, consistency, and fairness.

CONCLUSION

For the foregoing reasons, Keffer Development Services, LLC respectfully requests that the Judicial Panel on Multidistrict Litigation grant its Motion to Transfer and Consolidate all related actions for coordinated pretrial proceedings pursuant to 28 U.S.C. § 1407. These actions involve common factual and legal issues, are in the early stages of litigation, and are best suited for consolidation in the United States District Court for the Eastern District of Michigan. Centralization in that forum will promote the just and efficient conduct of the litigation by eliminating duplicative discovery, avoiding inconsistent pretrial rulings, reducing litigation costs, and preserving judicial and party resources. Accordingly, transfer to the Eastern District of Michigan is not only appropriate, but essential to ensure fairness, consistency, and efficiency in managing this complex and wide-reaching litigation.

Dated: June 5, 2025

Respectfully submitted,

**DILLON, MCCANDLESS, KING,
COULTER & GRAHAM LLP**

By: /s/ Thomas W. King, III

Thomas W. King, III

PA I.D. No. 21580

Jordan P. Shuber

PA I.D. No. 317823

Carl A. Fejko

PA I.D. No. 331216

Kyle S. Uhlman

CA I.D. No. 302292

128 West Cunningham Street

Butler, PA 16001

Telephone: 724-283-2200

Facsimile: 724-283-2298

TKing@dmkcg.com

*Attorneys for Defendant Keffer
Development Services, LLC*

“Exhibit A”

**BEFORE THE
UNITED STATES JUDICIAL PANEL ON
MULTIDISTRICT LITIGATION**

**IN RE: KEFFER DEVELOPMENT
SERVICES, LLC LITIGATION**

MDL DOCKET NO. _____

SCHEDULE OF ACTIONS

	Case Caption	Court	Civil Action No.	Judge
1	Plaintiff(s): JANE DOE 1 – 2, Consol Plaintiff(s): JANE DOE 25- 10855 1-53, McKenzie Johnson, Sarah Caldarola, Jenna Schilling, JANE ROE 25- 10870 CLF 001, JANE DOE 25- 10876, JANE DOE 25- 10951, JANE DOE 25-10946 1-11, JANE DOE 25- 10988 1-3, JANE DOE 25-10999, Defendant(s): MATTHEW	EASTERN DISTRICT OF MICHIGAN, Southern Division	2:25-cv-10806	Honorable Judge Mark A. Goldsmith

	WEISS; the REGENTS OF THE UNIVERSITY OF MICHIGAN; the UNIVERSITY OF MICHIGAN; KEFFER DEVELOPMENT SERVICES, LLC,			
2	Plaintiff(s): JANE DOE 1-53, McKenzie Johnson, Sarah Caldarola, Jenna Schilling, Defendant(s): MATTHEW WEISS; the REGENTS OF THE UNIVERSITY OF MICHIGAN; the UNIVERSITY OF MICHIGAN; KEFFER DEVELOPMENT SERVICES, LLC	EASTERN DISTRICT OF MICHIGAN, Southern Division	2:25-cv-10855 CONSOLIDATED AT 2:25-cv-10806	Honorable Judge Mark A. Goldsmith
3	Plaintiff(s): JANE DOE, Jane Doe 2, Jane Doe 3 Defendant(s): MATTHEW WEISS; the REGENTS OF THE UNIVERSITY OF MICHIGAN; the UNIVERSITY OF MICHIGAN; KEFFER	EASTERN DISTRICT OF MICHIGAN, Southern Division	2:25-cv-10988 CONSOLIDATED AT 2:25-cv-10806	Honorable Judge Mark A. Goldsmith

	DEVELOPMENT SERVICES, LLC			
4	<p>Plaintiff(s): JANE DOE obo herself and others similarly situated</p> <p>Defendant(s): THE UNIVERSITY OF MICHIGAN BOARD OF REGENTS; KEFFER DEVELOPMENT SERVICES, LLC, and MATTHEW WEISS</p>	EASTERN DISTRICT OF MICHIGAN, Southern Division	<p>2:25-cv-10951</p> <p>CONSOLIDATED AT 2:25-cv-10806</p>	Honorable Judge Mark A. Goldsmith
5	<p>Plaintiff(s): JANE DOE obo herself and others similarly situated</p> <p>Defendant(s): THE UNIVERSITY OF MICHIGAN BOARD OF REGENTS; KEFFER DEVELOPMENT SERVICES, LLC, and MATTHEW WEISS</p>	EASTERN DISTRICT OF MICHIGAN, Southern Division	<p>2:25-cv-10876</p> <p>CONSOLIDATED AT 2:25-cv-10806</p>	Honorable Judge Mark A. Goldsmith
6	<p>Plaintiff(s): STUDENT DOE 1, obo herself and others similarly situated</p> <p>Defendant(s): THE UNIVERSITY OF MICHIGAN</p>	EASTERN DISTRICT OF MICHIGAN, Southern Division	<p>2:25-cv-10999</p> <p>CONSOLIDATED AT 2:25-cv-10806</p>	Honorable Judge Mark A. Goldsmith

	BOARD OF REGENTS; KEFFER DEVELOPMENT SERVICES, LLC, and MATTHEW WEISS			
7	<p>Plaintiff(s): JANE DOE 1, JANE DOE 2, JANE DOE 3, JANE DOE 4, JANE DOE 5, JANE DOE 6, JANE DOE 7, JANE DOE 8, JANE DOE 9, JANE DOE 10, and JANE DOE 11</p> <p>Defendant(s): THE REGENTS OF THE UNIVERSITY OF MICHIGAN; the UNIVERSITY OF MICHIGAN; KEFFER DEVELOPMENT SERVICES, LLC, and MATTHEW WEISS</p>	EASTERN DISTRICT OF MICHIGAN, Southern Division	2:25-cv-10946 CONSOLIDATED AT 2:25-cv-10806	Honorable Judge Mark A. Goldsmith
8	<p>Plaintiff(s): JANE ROE CLF 001</p> <p>Defendant(s): MATTHEW WEISS; THE REGENTS OF THE UNIVERSITY OF MICHIGAN; THE UNIVERISTY OF</p>	EASTERN DISTRICT OF MICHIGAN, Southern Division	2:25-cv-10870 CONSOLIDATED AT 2:25-cv-10806	Honorable Judge Mark A. Goldsmith

	MICHIGAN; KEFFER DEVELOPMENT SERVICES, LLC			
9	Plaintiff(s): JANE DOE 1 Defendant(s): MATTHEW WEISS; LOYALA UNIVERSITY CHICAGO, AND KEFFER DEVELOPMENT SERVICES, LLC	NORTHERN DISTRICT OF ILLINOIS, Chicago	1:25-cv-04233	Honorable Judge Matthew F. Kennelly
10	Plaintiff(s): JANE DOE 1 Defendant(s): MATTHEW WEISS, MALONE UNIVERSITY and KEFFER DEVELOPMENT, LLC	NORTHERN DISTRICT OF OHIO, Akron	5:25-cv-00827	Honorable Chief District Judge Sara Loi
11	Plaintiff(s): JANE DOE 1 Defendant(s): MATTHEW WEISS, CALIFORNIA STATE UNIVERSITY, SAN BERNARDINO, BOARD OF TRUSTEES OF THE CALIFORNIA STATE UNIVERSITY, and KEFFER	CENTRAL DISTRICT OF CALIFORNIA, Eastern Division – Riverside	5:25-cv-00997	Honorable Judge Hernan D. Vera

	DEVELOPMENT SERVICES, LCC			
12	Plaintiff(s): JANE DOES 1 and 2 Defendant(s): MATTHEW WEISS, HIGH POINT UNIVERSITY, and KEFFER DEVELOPMENT SERVICES, LLC	MIDDLE DISTRICT OF NORTH CAROLINA	1:25-cv-00303	Honorable Judge Catherine C. Eagles
13	Plaintiff(s): JANE DOE Defendant(s): MATTHEW WEISS; the TRUSTEES OF SIMMONS UNIVERSITY; SIMMONS UNIVERSITY; and KEFFER DEVELOPMENT SERVICES, LLC	DISTRICT COURT OF MASSACHUSETTS, Boston	1:25-cv-11151	Honorable Judge Julia E. Kobick

Dated: June 9, 2025

Respectfully submitted,

**DILLON, MCCANDLESS, KING,
COULTER & GRAHAM LLP**

By: /s/ Thomas W. King, III

Thomas W. King, III

PA I.D. No. 21580

Jordan P. Shuber

PA I.D. No. 317823

Carl A. Fejko

PA I.D. No. 331216

Kyle S. Uhlman

CA I.D. No. 302292

128 West Cunningham Street

Butler, PA 16001

Telephone: 724-283-2200

Facsimile: 724-283-2298

TKing@dmkcg.com

Attorneys for Defendant Keffer
Development Services, LLC

**BEFORE THE
UNITED STATES JUDICIAL PANEL ON
MULTIDISTRICT LITIGATION**

**IN RE: KEFFER DEVELOPMENT
SERVICES, LLC LITIGATION**

MDL DOCKET NO. _____

PROOF OF SERVICE

Pursuant to Rule 4.1(a) of the Rules of Procedure of the United States Judicial Panel on Multidistrict Litigation, I hereby certify that on this June 5, 2025, I caused to be filed with the Clerk of the Court using the Judicial Panel on Multidistrict Litigation's CM/ECF system: served true and correct copies of the following documents:

- (1) Keffer Development Services, LLC's Motion to Transfer Related Cases for Consolidated Pretrial Proceedings Pursuant to 28 U.S.C. § 1407;
- (2) Brief in Support of Keffer Development Services, LLC's Motion to Transfer Related Cases for Consolidated Pretrial Proceedings Pursuant to 28 U.S.C. § 1407;
- (3) Schedule of Actions, including docket sheets and complaints for all related actions; and
- (4) Proof of Service

I further certify that copies of the foregoing were served on all counsel and on the Clerk of the Court of each proposed transferor court, by email or First Class Mail, as follows:

Dated: June 9, 2025

Respectfully submitted,

**DILLON, MCCANDLESS, KING,
COULTER & GRAHAM LLP**

By: /s/ Thomas W. King, III
Thomas W. King, III
PA I.D. No. 21580
Jordan P. Shuber
PA I.D. No. 317823
Carl A. Fejko

PA I.D. No. 331216
 Kyle S. Uhlman
 CA I.D. No. 302292

128 West Cunningham Street
 Butler, PA 16001
 Telephone: 724-283-2200
 Facsimile: 724-283-2298
TKing@dmkcg.com

*Attorneys for Defendant Keffer
 Development Services, LLC*

COURT CLERKS	
United States District Court for the Eastern District of Michigan Clerk's Office Theodore Levin U.S. Courthouse 231 W. Lafayette Blvd., Room 599 Detroit, Michigan 48226	United States District Court for the Northern District of Ohio Clerk's Office John F. Seiberling Federal Building & U.S. Courthouse 2 South Main Street Akron, Ohio 44308
United States District Court for the District of Massachusetts Clerk's Office 1 Courthouse Way Boston, Massachusetts 02210	United States District Court for the Central District of California Clerk's Office 3470 12 th Street Riverside, California 92501
United States District Court for the Middle District of North Carolina Clerk's Office 324 W. Market Street Suite 400 Greensboro, North Carolina 27401	United States District Court for the Northern District of Illinois Clerk's Office 219 S. Dearborn Street Chicago, Illinois 60604-1702
COUNSEL/PARTIES Doe 1 et al v. Weiss et al No. 2:25-cv-10806 Eastern District of Michigan (Detroit) Plaintiff Jane Doe 1 - 2	

<p>Aimee Wagstaff Wagstaff Law Firm, PC 940 N. Lincoln St. Denver, CO 80203 303-376-6360 Email: awagstaff@wagstafflawfirm.com</p>	<p>Bart Cohen Bailey Glasser LLP 1622 Locust St. Philadelphia, PA 19103 267-973-4855 Email: bcohen@baileyglasser.com</p>
<p>Benjamin Gillig Wagstaff Law Firm 940 N. Lincoln Street Denver, CO 80203 303-376-6360 Email: bgillig@wagstafflawfirm.com</p>	<p>Brian A Glasser Bailey & Glasser 1055 Thomas Jefferson Street NW Suite 540 Washington, DC 20007 304-345-6555 Fax: 304-342-1110 Email: bglasser@baileyglasser.com</p>
<p>Bryce Thomas Hensley Stinar Gould Grieco & Hensley, PLLC IL 101 N Wacker Drive Suite 100 Chicago Chicago, IL 60606 847-890-1171 Email: bryce@sgghlaw.com</p>	<p>D. Todd Mathews Bailey & Glasser PO Box 993 Maryville, IL 62062 618-520-3342 Fax: 304-342-1110 Email: tmathews@baileyglasser.com</p>
<p>David L. Selby, II Bailey & Glasser 3000 Riverchase Galleria Suite 905 Birmingham, AL 35244 205-988-9253 Fax: 205-733-4896 Email: dselby@baileyglasser.com</p>	<p>Erik Johnson Stinar, Gould, Grieco & Hensley Litigation 550 W. Merrill St. Suite 240 Birmingham, MI 48009 248-221-8561 Email: erik@sgghlaw.com</p>
<p>John W Barrett Bailey & Glasser 209 Capitol Street Charleston, WV 25301 304-345-6555 Fax: 304-342-1110 Email: jbarrett@baileyglasser.com</p>	<p>Jonathan R. Marko Marko Law, PLLC 220 W. Congress 4th Floor Detroit, MI 48226 313-777-7529 Fax: 313-470-2011 Email: jon@markolaw.com</p>
<p>Katherine E. Charonko Bailey & Glasser 209 Capitol Street Charleston, WV 25301 304-345-6555</p>	<p>Michael R. Grieco Stinar Gould Grieco & Hensley 101 N. Wacker Drive Suite 100 Chicago, IL 60606</p>

Fax: 304-342-1110 Email: kcharonko@baileyglasser.com	312-728-7444 Fax: 313-221-9950 Email: mike@sgghlaw.com
Patrick C. Lannen Stinar Gould Grieco & Hensley 550 W. Merrill Ste. 240 Birmingham, MI 48009 248-232-7409 Email: patrick@sgghlaw.com	Yana A. Hart Clarkson Law Firm 22525 Pacific Coast Highway Malibu, CA 90265 213-788-4050 Email: yhart@clarksonlawfirm.com
Parker G. Stinar Stinar Gould Grieco & Hensley 101 N. Wacker Dr., Ste. 100 Chicago, IL 60606 312-728-7444 Email: parker@sgghlaw.com	
Doe 1 et al v. Weiss et al No. 2:25-cv-10806 Eastern District of Michigan (Detroit) Plaintiff Jane Doe, 1-53 Consolidated from 25-10855	
Brendan John Childress Hurwitz Law PLLC 617 Detroit St. Suite 125 Ann Arbor, MI 48104 248-933-5121 Email: brendan@hurwitzlaw.com	Jonathan R. Marko (See above for address)
Noah S. Hurwitz Hurwitz Law PLLC 1514 Creal Cres Ann Arbor, MI 48103 734-645-5263 Email: noah@hurwitzlaw.com	Yana A. Hart (See above for address)
Erik Johnson (See above for address)	
Doe 1 et al v. Weiss et al No. 2:25-cv-10806 Eastern District of Michigan (Detroit) Plaintiff McKenzie Johnson Consolidated from 25-10855	
Brendan John Childress (See above for address)	Noah S. Hurwitz (See above for address)
Erik Johnson (See above for address)	
Doe 1 et al v. Weiss et al	

No. 2:25-cv-10806 Eastern District of Michigan (Detroit) Plaintiff Sarah Caldarola Consolidated from 25-10855	
Noah S. Hurwitz (See above for address)	Erik Johnson (See above for address)
Doe 1 et al v. Weiss et al No. 2:25-cv-10806 Eastern District of Michigan (Detroit) Plaintiff Jenna Schilling Consolidated from 25-10855	
Noah S. Hurwitz (See above for address)	Erik Johnson (See above for address)
Doe 1 et al v. Weiss et al No. 2:25-cv-10806 Eastern District of Michigan (Detroit) Plaintiff JANE ROE CLF 001 Consolidated from 25-10870	
Bryan Paul Thompson Clarkson Law Firm, P.C. 875 North Michigan Avenue 31st Floor Chicago, IL 60611 312-267-0061 Email: bthompson@clarksonlawfirm.com	Ryan Clarkson Clarkson Law Firm, P.C. Clarkson Law Firm, P.C. 22525 Pacific Coast Highway Malibu, CA 90265 213-788-4050 Email: rclarkson@clarksonlawfirm.com
Yana A. Hart (See above for address)	Erik Johnson (See above for address)
Doe 1 et al v. Weiss et al No. 2:25-cv-10806 Eastern District of Michigan (Detroit) Plaintiff Jane Doe, Consolidated from 25-10876	
David H. Fink Fink Bressack PLLC 38500 Woodward Ave. Suite 350 Bloomfield Hills, MI 48304 248-971-2500 Fax: 248-971-2600 Email: dfink@finkbressack.com	Nathan J. Fink Fink Bressack PLLC 38500 Woodward Avenue Ste 350 Bloomfield Hills, MI 48304 248-971-2500 Email: nfink@finkbressack.com
Yana A. Hart (See above for address)	Erik Johnson (See above for address)
Doe 1 et al v. Weiss et al No. 2:25-cv-10806 Eastern District of Michigan (Detroit) Plaintiff Jane Doe, Consolidated from 25-10951	
David H. Fink	James Gerard Stranch, IV

(See above for address)	Stranch, Jennings & Garvey, PLLC 223 Rosa L. Parks Avenue Freedom Building Ste 200 Nashville, TN 37203 615-254-8801 Fax: 615-250-3937 Email: gstranch@stranchlaw.com
Nathan J. Fink (See above for address)	Yana A. Hart (See above for address)
Erik Johnson (See above for address)	
No. 2:25-cv-10806 Eastern District of Michigan (Detroit) Plaintiff Jane Doe 1-11, Consolidated from 25-10946	
Beth M. Rivers Pitt McGehee Palmer & Rivers 117 W. Fourth Street Suite 200 Royal Oak, MI 48067-3804 248-398-9800 Email: brivers@pittlawpc.com	Danielle Young Canepa Pitt McGehee Palmer Bonanni & Rivers PC 117 W. 4th Street Suite 200 Royal Oak, MI 48067 248-398-9800 Email: dcanepa@pittlawpc.com
Jason J. Thompson Sommers Schwartz, P.C. One Towne Square Suite 1700 Southfield, MI 48076 248-355-0300 Fax: 248-436-8453 Email: jthompson@sommerspc.com	Kevin Michael Carlson Pitt McGehee Palmer & Rivers PC 117 West Fourth Street Suite 200 Royal Oak, MI 48067 248-398-9800 Email: kcarlson@pittlawpc.com
Lisa M. Esser Sommers Schwartz, P.C. One Towne Square Ste 1700 Southfield, MI 48076 248-355-0300 Email: lesser@sommerspc.com	Matthew G. Curtis Sommers Schwartz, P.C. One Towne Square 17th Floor Southfield Southfield, MI 48076 248-746-4038 Fax: 248-936-2124 Email: mcurtis@sommerspc.com
Megan Bonanni Pitt, McGehee, 117 W. Fourth Street Suite 200	Richard L. Groffsky Sommers Schwartz One Towne Center Ste 1700

Royal Oak, MI 48067-3804 248-398-9800 Email: mbonanni@pittlawpc.com	Southfield, MI 48076 248-746-4028 Email: rgroffsky@sommerspc.com
Sara Mickovic Sommers Schwartz, P.C. 1 Towne Square #1700 Southfield, MI 48076 248-916-2730 Email: smickovic@sommerspc.com	Yana A. Hart (See above for address)
Erik Johnson (See above for address)	
No. 2:25-cv-10806 Eastern District of Michigan (Detroit) Plaintiff Jane Doe 1-3, Consolidated from 25-10988	
Robert J. Lantzy Buckfire & Buckfire 29000 Inkster Road Ste. 150 Southfield, MI 48034 248-569-4646 Email: robert@buckfirelaw.com	Yana A. Hart (See above for address)
Erik Johnson (See above for address)	
No. 2:25-cv-10806 Eastern District of Michigan (Detroit) Plaintiff Jane Doe 1-3, Consolidated from 25-10999	
Gary M. Klinger Milberg Coleman Bryson Phillips Grossman PLLC 227 W. Monroe Street Suite 2100 Chicago, IL 60606 866-252-0878 Email: gklinger@milberg.com	James Joseph Pizzirusso Hausfeld LLP 1200 17th Street, NW Suite 600 Washington, DC 20036 202-540-7200 Fax: 202-540-7201 Email: jpizzirusso@hausfeld.com
Mariya Weekes Milberg Coleman Bryson Phillips Grossman, PLLC 201 Sevilla Avenue, 2nd Floor Coral Gables, FL 33134 954-647-1866 Email: mweekes@milberg.com	Steven M. Nathan Hausfeld LLP NYC 33 Whitehall Street Ste 14th Floor New York, NY 10004 646-357-1100 Fax: 212-202-4322 Email: snathan@hausfeld.com

Yana A. Hart (See above for address)	Erik Johnson (See above for address)
No. 2:25-cv-10806 And 2:25-cv-10855, 2:25-cv-10988, 2:25-cv-10951, 2:25-cv-10876, 2:25-cv-10999, 2:25-cv-10946, 2:25-cv-10870 Eastern District of Michigan (Detroit) Defendant Matthew Weiss	
None listed ¹	
No. 2:25-cv-10806 And 2:25-cv-10855, 2:25-cv-10988, 2:25-cv-10951, 2:25-cv-10876, 2:25-cv-10999, 2:25-cv-10946, 2:25-cv-10870 Eastern District of Michigan (Detroit) Defendant the Regents of the University of Michigan	
Daniel B. Tukel Butzel Long 201 West Big Beaver Road Suite 1200 Troy, MI 48084 313-225-7047 Email: tukel@butzel.com	Sheldon H. Klein Butzel 201 West Big Beaver Road Suite 1200 Troy, MI 48084 248-258-1414 Fax: 248-258-1439 Email: klein@butzel.com
No. 2:25-cv-10806 And 2:25-cv-10855, 2:25-cv-10988, 2:25-cv-10951, 2:25-cv-10876, 2:25-cv-10999, 2:25-cv-10946, 2:25-cv-10870 Eastern District of Michigan (Detroit) Defendant the University of Michigan	
Daniel B. Tukel (See above for address)	Sheldon H. Klein (See above for address)
No. 2:25-cv-10806 And 2:25-cv-10855, 2:25-cv-10988, 2:25-cv-10951, 2:25-cv-10876, 2:25-cv-10999, 2:25-cv-10946, 2:25-cv-10870 Eastern District of Michigan (Detroit) Defendant Keffer Development Services, LLC	
Carl Andrew Fejko	Jordan P. Shuber

¹ No contact information available for Defendant Matthew Weiss

Dillon McCandless King Coulter Graham, LLP Civil Practice 128 West Cunningham St. Butler, PA 16001 724-822-2148 Email: cfejko@dmkcg.com	Dillon McCandless King Coulter & Graham, LLP 128 West Cunningham Street Butler, PA 16001 724-283-2200 Fax: 724-283-2298 Email: jshuber@dmkcg.com
Thomas W. King, III Dillon McCandless King Coulter & Graham, LLP 128 West Cunningham Street Butler, PA 16001 724-283-2200 Email: tking@dmkcg.com	
COUNSEL/PARTIES No. 1:25-cv-04233 Northern District of Illinois Plaintiff Jane Doe	
Jason J Thompson Sommers Schwartz, Pc 1 Towne Square, Suite 1700 Southfield, MI 48076 (248) 355-0300 Fax: Not a member Email: jthompson@sommerspc.com LEAD ATTORNEY	Jacob Mayer Podell Wallace Miller 150 N Wacker Dr Chicago, IL 60606 (312) 261-6193 Fax: Not a member Email: jpodell@wallacemiller.com
Matthew G Curtis, Male Sommers Schwartz, P.C. One Towne Square 17th Floor Southfield Southfield, MI 48076 248-746-4038 Fax: 248-936-2124 Email: mcurtis@sommerspc.com PRO HAC VICE	Megan A. Bonanni Pitt McGehee Palmer Bonanni & Rivers, PC 117 W. Fourth Street, Suite 200 Suite 200 Royal Oak, MI 48067 248-398-9800 Fax: 248-268-7996 Email: mbonanni@pittlawpc.com
Richard Groffsky Sommers Schwartz, P.C. One Towne Square, 17th Floor Southfield, MI 48076 (248) 355-0300 Fax: Pro Hac Vice Email: rgroffsky@s	Edward A. Wallace Wallace Miller 150 N Wacker Ste 1100 Chicago, IL 60606 312-261-6193 Fax: 312-275-8174 Email: eaw@wallacemiller.com

No. 1:25-cv-04233 Northern District of Illinois Defendant Matthew Weiss	
None listed ²	
No. 1:25-cv-04233 Northern District of Illinois Defendant Loyola University Chicago	
Mary S DiRago Troutman Pepper Locke LLP 111 South Wacker Drive Suite 4100 Chicago, IL 60606 312-759-1926 Fax: 312-759-1939 Email: molly.dirago@troutman.com	
No. 1:25-cv-04233 Northern District of Illinois Defendant Keffer Development Services, LLC	
None listed on docket Thomas W. King, III Dillon McCandless King Coulter & Graham, LLP 128 West Cunningham Street Butler, PA 16001 724-283-2200 Email: tking@dmkcg.com (admission forthcoming)	Jordan P. Shuber Dillon McCandless King Coulter & Graham, LLP 128 West Cunningham Street Butler, PA 16001 724-283-2200 Fax: 724-283-2298 Email: jshuber@dmkcg.com (admission forthcoming)
COUNSEL/PARTIES No. 5:25-cv-00827 Northern District of Ohio (Akron) Plaintiff Jane Doe	
Anna R. Caplan Barkan Meizlish DeRose Cox - Columbus Ste. 210 4200 Regent Street Columbus, OH 43082 614-221-4221 Fax: 614-744-2300 Email: acaplan@barkanmeizlish.com	Jason J. Thompson Sommers Schwartz - Southfield Ste. 1700 One Towne Square Southfield, MI 48076 248-355-0300 Email: jthompson@sommerspc.com PRO HAC VICE
Kevin M. Carlson	Lisa M. Esser

² No contact information available for Defendant Matthew Weiss

Pitt McGehee Palmer Bonanni & Rivers - Royal Oak Ste. 200 117 West Fourth Street Royal Oak, MI 48067 248-398-9800 Fax: 248-298-7996 Email: kcarlson@pittlawpc.com PRO HAC VICE	Sommers Schwartz - Southfield Ste. 1700 One Towne Square Southfield, MI 48076 248-355-0300 Email: lesser@sommerspc.com PRO HAC VICE
Matthew G. Curtis Sommers Schwartz - Southfield 17th Floor One Towne Square Southfield, MI 48076 248-746-4038 Fax: 248-936-2124 Email: mcurtis@sommerspc.com PRO HAC VICE	Megan A. Bonanni Pitt McGehee Palmer & Rivers - Royal Oak Ste. 200 117 West Fourth Street Royal Oak, MI 48067 248-398-9800 Fax: 248-268-7996 Email: mbonanni@pittlawpc.com PRO HAC VICE
Richard L. Groffsky Sommers Schwartz - Southfield Ste. 1700 One Towne Center Southfield, MI 48076 248-746-4028 Email: rgroffsky@sommerspc.com PRO HAC VICE	Robert E. DeRose , II Barkan Meizlish DeRose Cox Ste. 210 4200 Regent Street Columbus, OH 43219 614-221-4221 Fax: 614-744-2300 Email: bderose@barkanmeizlish.com
No. 5:25-cv-00827 Northern District of Ohio (Akron) Defendant Matthew Weiss	
None listed ³	
No. 5:25-cv-00827 Northern District of Ohio (Akron) Defendant Malone University	
Melissa Bilancini Baker & Hostetler - Cleveland Ste. 2000 127 Public Square Cleveland, OH 44114 216-621-0200 Fax: 216-696-0740 Email: mbilancini@bakerlaw.com	
No. 5:25-cv-00827	

³ No contact information available for Defendant Matthew Weiss

Northern District of Ohio (Akron) Defendant Keffer Development Services, LLC	
None listed on docket Thomas W. King, III (See above for Address) <i>-admission forthcoming</i>	Jordan P. Shuber (See above for Address) <i>-admission forthcoming</i>
COUNSEL/PARTIES No. 5:25-cv-00997 Central District of California (Eastern Division – Riverside) Plaintiff Jane Doe 1	
Yana A. Hart Clarkson Law Firm PC 22525 Pacific Coast Highway Malibu, CA 90265 213-788-4050 Fax: 213-788-4070 Email: yhart@clarksonlawfirm.com LEAD ATTORNEY	Bryan Paul Thompson Clarkson Law Firm, P.C. 22525 Pacific Coast Highway Malibu, CA 90265 312-267-0061 Fax: 213-788-4070 Email: bthompson@clarksonlawfirm.com
Jason J. Thompson Sommers Schwatz PC One Towne Square 17th Floor Southfield, MI 48076 248-355-0300 Fax: 248-746-4001 Email: jthompson@sommerspc.com PRO HAC VICE	Megan A Bonanni Pitt McGehee Palmer Bonanni and Rivers P.C. 117 W. Fourth Street Suite 200 Royal Oak, MI 48067 248-398-9800 Fax: 248-268-7996 Email: mbonanni@pittlawpc.com PRO HAC VICE
Ryan J. Clarkson Clarkson Law Firm PC 22525 Pacific Coast Highway Malibu, CA 90265 213-788-4050 Fax: 213-788-4070 Email: rclarkson@clarksonlawfirm.com	
No. 5:25-cv-00997 Central District of California (Eastern Division – Riverside) Defendant Matthew Weiss	
None listed ⁴	
No. 5:25-cv-00997 Central District of California (Eastern Division – Riverside) Defendant The Board of Trustees of the California State University	

⁴ No contact information available for Defendant Matthew Weiss

Amy Thomas Brantly Kesselman Brantly Stockinger LLP 1230 Rosecrans Avenue Suite 400 Manhattan Beach, CA 90266 310-307-4555 Fax: 310-307-4570 Email: Abrantly@kbslaw.com	David W. Kesselman Kesselman Brantly Stockinger LLP 1230 Rosecrans Avenue Suite 400 Manhattan Beach, CA 90266 310-307-4555 Fax: 310-307-4570 Email: dkesselman@kbslaw.com
Mark Paluch Kesselman Brantly Stockinger LLP 1230 Rosecrans Ave., Suite 400 Manhattan Beach, CA 90266 310-307-4555 Fax: 310-307-4570 Email: mpaluch@kbslaw.com	
No. 5:25-cv-00997 Central District of California (Eastern Division – Riverside) Defendant The Board of Trustees of the California State University	
Amy Thomas Brantly (See above for address)	David W. Kesselman (See above for address)
Mark Paluch (See above for address)	
No. 5:25-cv-00997 Central District of California (Eastern Division – Riverside) Defendant Keffer Development Services, LLC	
Kyle S. Uhlman DILLON McCANDLESS KING COULTER & GRAHAM 128 W. Cunningham Street Butler, PA 16001 724-283-2200 Email: kuhlman@dmkcg.com	
COUNSEL/PARTIES No. 1:25-cv-00303 North Carolina Middle District (NCMD) Plaintiff Jane Doe 1	
JAMES J. MILLS BURNS DAY & PRESNELL, P.A. POB 10867 RALEIGH, NC 27605 919-782-1441 Fax: 919-782-2311 Email: jmills@bdppa.com LEAD ATTORNEY	KEVIN CARLSON PITT MCGEHEE PALMER BONANNI & RIVERS PC 117 WEST FOURTH STREET SUITE 200 ROYAL OAK, MI 48067 248-398-9800 Fax: 248-298-7996 Email: kcarlson@pittlawpc.com

	LEAD ATTORNEY
MEGAN A BONANNI PITT MCGEHEE PALMER BONANNI & RIVERS 117 W. FOURTH STREET SUITE 200 ROYAL OAK, MI 48067 248-398-9800 Fax: 248-268-7996 Email: mbonanni@pittlawpc.com LEAD ATTORNEY	JASON THOMPSON SOMMERS SCHWARTZ, P.C. ONE TOWNE SQUARE SUITE 1700 Southfield, MI 48076 248-355-0300 Email: jthompson@sommerspc.com
LISA MICHELLE ESSER SOMMERS SCHWARTZ, P.C. ONE TOWNE SQUARE STE 1700 SOUTHFIELD, MI 48076 248-355-0300 Email: lesser@sommerspc.com	MATTHEW G CURTIS SOMMERS SCHWARTZ, PC ONE TOWNE SQUARE STE 17TH FLOOR SOUTHFIELD, MI 48076 248-746-4038 Fax: 248-936-2124 Email: mcurtis@sommerspc.com
RICHARD GROFFSKY SOMMERS SCHWARTZ, P.C. ONE TOWNE CENTER STE 1700 SOUTHFIELD, MI 48076 248-746-4028 Email: rgroffsky@gmail.com	
No. 1:25-cv-00303 North Carolina Middle District (NCMD) Plaintiff Jane Doe 2	
JAMES J. MILLS (See above for address) LEAD ATTORNEY	KEVIN CARLSON (See above for address) LEAD ATTORNEY
MEGAN A BONANNI (See above for address) LEAD ATTORNEY	JASON THOMPSON (See above for address)
LISA MICHELLE ESSER (See above for address)	MATTHEW G CURTIS (See above for address)
RICHARD GROFFSKY (See above for address)	
No. 1:25-cv-00303 North Carolina Middle District (NCMD) Defendant High Point University	
Registered Agent: Steven Bradford Calloway	

High Point University 1 University Pkwy High Point, NC 27268	
No. 1:25-cv-00303 North Carolina Middle District (NCMD) Defendant Matthew Weiss	
None listed ⁵	
No. 1:25-cv-00303 North Carolina Middle District (NCMD) Defendant Keffer Development Services, LLC	
None listed on docket Thomas W. King, III (See above for Address) <i>-admission forthcoming</i>	Jordan P. Shuber (See above for Address) <i>-admission forthcoming</i>
No. 1:25-cv-11151 District of Massachusetts (Boston) Plaintiff Jane Doe	
Paula S. Bliss Justice Law Collaborative, LLC 210 Washington Street North Easton, MA 02356 508-230-2700 Email: paula@justicelc.com	
No. 1:25-cv-11151 District of Massachusetts (Boston) Defendant Matthew Weiss	
None listed ⁶	
No. 1:25-cv-11151 District of Massachusetts (Boston) Defendant Simmons University	
None listed Simmons University 300 The Fenway Boston, MA 02115 ⁷	
No. 1:25-cv-11151 District of Massachusetts (Boston) Defendant The Trustees of Simmons University	
None listed Simmons University 300 The Fenway	

⁵ No contact information available for Defendant Matthew Weiss

⁶ No contact information available for Defendant Matthew Weiss

⁷ No address listed on the court docket, Mailing address of University added for Service

Boston, MA 02115	
No. 1:25-cv-11151 District of Massachusetts (Boston) Defendant Keffer Development Services, LLC	
None listed on docket Thomas W. King, III (See above for Address) <i>-admission forthcoming</i>	Jordan P. Shuber (See above for Address) <i>-admission forthcoming</i>

**U.S. District Court
Eastern District of Michigan (Detroit)
CIVIL DOCKET FOR CASE #: 2:25-cv-10806-MAG-EAS**

Doe 1 et al v. Weiss et al
Assigned to: District Judge Mark A. Goldsmith
Referred to: Magistrate Judge Elizabeth A. Stafford
Demand: \$9,999,000
Cause: 28:1345 Property Damage

Date Filed: 03/21/2025
Jury Demand: Plaintiff
Nature of Suit: 370 Other Fraud
Jurisdiction: Federal Question

Plaintiff

Jane Doe 1

represented by **Aimee Wagstaff**
Wagstaff Law Firm, PC
940 N. Lincoln St.
Denver, CO 80203
303-376-6360
Email: awagstaff@wagstafflawfirm.com
ATTORNEY TO BE NOTICED

Bart Cohen
Bailey Glasser LLP
1622 Locust St.
Philadelphia, PA 19103
267-973-4855
Email: bcohen@baileyglasser.com
ATTORNEY TO BE NOTICED

Benjamin Gillig
Wagstaff Law Firm
940 N. Lincoln Street
Denver, CO 80203
303-376-6360
Email: bgillig@wagstafflawfirm.com
ATTORNEY TO BE NOTICED

Brian A Glasser
Bailey & Glasser
1055 Thomas Jefferson Street NW
Suite 540
Washington, DC 20007
304-345-6555
Fax: 304-342-1110
Email: bglasser@baileyglasser.com
ATTORNEY TO BE NOTICED

Bryce Thomas Hensley
Stinar Gould Grieco & Hensley, PLLC
IL
101 N Wacker Drive
Suite 100

Chicago
Chicago, IL 60606
847-890-1171
Email: bryce@sgghlaw.com
ATTORNEY TO BE NOTICED

D. Todd Mathews

Bailey & Glasser
PO Box 993
Maryville, IL 62062
618-520-3342
Fax: 304-342-1110
Email: tmathews@baileyglasser.com
ATTORNEY TO BE NOTICED

David L. Selby , II

Bailey & Glasser
3000 Riverchase Galleria
Suite 905
Birmingham, AL 35244
205-988-9253
Fax: 205-733-4896
Email: dselby@baileyglasser.com
ATTORNEY TO BE NOTICED

Erik Johnson

Stinar, Gould, Grieco & Hensley
Litigation
550 W. Merril St.
Suite 240
Birmingham, MI 48009
248-221-8561
Email: erik@sgghlaw.com
ATTORNEY TO BE NOTICED

John W Barrett

Bailey & Glasser
209 Capitol Street
Charleston, WV 25301
304-345-6555
Fax: 304-342-1110
Email: jbarrett@baileyglasser.com
ATTORNEY TO BE NOTICED

Jonathan R. Marko

Marko Law, PLLC
220 W. Congress
4th Floor
Detroit, MI 48226
313-777-7529
Fax: 313-470-2011
Email: jon@markolaw.com
ATTORNEY TO BE NOTICED

Katherine E. Charonko

Bailey & Glasser

209 Capitol Street

Charleston, WV 25301

304-345-6555

Fax: 304-342-1110

Email: kcharonko@baileyglasser.com

*ATTORNEY TO BE NOTICED***Michael R. Grieco**

Stinar Gould Grieco & Hensley

101 N. Wacker Drive

Suite 100

Chicago, IL 60606

312-728-7444

Fax: 313-221-9950

Email: mike@sgghlaw.com

*ATTORNEY TO BE NOTICED***Patrick C. Lannen**

Stinar Gould Grieco & Hensley

550 W. Merrill

Ste. 240

Birmingham, MI 48009

248-232-7409

Email: patrick@sgghlaw.com

*ATTORNEY TO BE NOTICED***Yana A. Hart**

Clarkson Law Firm

22525 Pacific Coast Highway

Malibu, CA 90265

213-788-4050

Email: yhart@clarksonlawfirm.com

*ATTORNEY TO BE NOTICED***Parker G. Stinar**

Stinar Gould Grieco & Hensley

101 N. Wacker Dr., Ste. 100

Chicago, IL 60606

312-728-7444

Email: parker@sgghlaw.com

*ATTORNEY TO BE NOTICED***Plaintiff****Jane Doe 2**represented by **Aimee Wagstaff**

(See above for address)

*ATTORNEY TO BE NOTICED***Bart Cohen**

(See above for address)

*ATTORNEY TO BE NOTICED***Benjamin Gillig**

(See above for address)
ATTORNEY TO BE NOTICED

Brian A Glasser
(See above for address)
ATTORNEY TO BE NOTICED

Bryce Thomas Hensley
(See above for address)
ATTORNEY TO BE NOTICED

D. Todd Mathews
(See above for address)
ATTORNEY TO BE NOTICED

David L. Selby , II
(See above for address)
ATTORNEY TO BE NOTICED

Erik Johnson
(See above for address)
ATTORNEY TO BE NOTICED

John W Barrett
(See above for address)
ATTORNEY TO BE NOTICED

Jonathan R. Marko
(See above for address)
ATTORNEY TO BE NOTICED

Katherine E. Charonko
(See above for address)
ATTORNEY TO BE NOTICED

Michael R. Grieco
(See above for address)
ATTORNEY TO BE NOTICED

Patrick C. Lannen
(See above for address)
ATTORNEY TO BE NOTICED

Yana A. Hart
(See above for address)
ATTORNEY TO BE NOTICED

Parker G. Stinar
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Jane Doe
1-53, Consolidated from 25-10855

represented by **Brendan John Childress**
Hurwitz Law PLLC

617 Detroit St.
Suite 125
Ann Arbor, MI 48104
248-933-5121
Email: brendan@hurwitzlaw.com
ATTORNEY TO BE NOTICED

Jonathan R. Marko
(See above for address)
ATTORNEY TO BE NOTICED

Noah S. Hurwitz
Hurwitz Law PLLC
1514 Creal Cres
Ann Arbor, MI 48103
734-645-5263
Email: noah@hurwitzlaw.com
ATTORNEY TO BE NOTICED

Yana A. Hart
(See above for address)
ATTORNEY TO BE NOTICED

Erik Johnson
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

McKenzie Johnson
Consolidated from 25-10855

represented by **Brendan John Childress**
(See above for address)
ATTORNEY TO BE NOTICED

Noah S. Hurwitz
(See above for address)
ATTORNEY TO BE NOTICED

Erik Johnson
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Sarah Caldarola
Consolidated from 25-10855

represented by **Noah S. Hurwitz**
(See above for address)
ATTORNEY TO BE NOTICED

Erik Johnson
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Jenna Schilling
Consolidated from 25-10855

represented by **Noah S. Hurwitz**
(See above for address)
ATTORNEY TO BE NOTICED

Erik Johnson

(See above for address)

ATTORNEY TO BE NOTICED

Plaintiff

JANE ROE CLF 001

Consolidated from 25-10870

represented by

Bryan Paul Thompson

Clarkson Law Firm, P.C.

875 North Michigan Avenue

31st Floor

Chicago, IL 60611

312-267-0061

Email: bthompson@clarksonlawfirm.com

ATTORNEY TO BE NOTICED

Ryan Clarkson

Clarkson Law Firm, P.C.

Clarkson Law Firm, P.C.

22525 Pacific Coast Highway

Malibu, CA 90265

213-788-4050

Email: rclarkson@clarksonlawfirm.com

ATTORNEY TO BE NOTICED

Yana A. Hart

(See above for address)

ATTORNEY TO BE NOTICED

Erik Johnson

(See above for address)

ATTORNEY TO BE NOTICED

Plaintiff

Jane Doe

Consolidated from 25-10876

represented by

David H. Fink

Fink Bressack PLLC

38500 Woodward Ave.

Suite 350

Bloomfield Hills, MI 48304

248-971-2500

Fax: 248-971-2600

Email: dfink@finkbressack.com

ATTORNEY TO BE NOTICED

Nathan J. Fink

Fink Bressack PLLC

38500 Woodward Avenue

Ste 350

Bloomfield Hills, MI 48304

248-971-2500

Email: nfink@finkbressack.com

ATTORNEY TO BE NOTICED

Yana A. Hart

(See above for address)

ATTORNEY TO BE NOTICED

Erik Johnson

(See above for address)

*ATTORNEY TO BE NOTICED***Plaintiff****Jane Doe***Consolidated from 25-10951*represented by **David H. Fink**

(See above for address)

*ATTORNEY TO BE NOTICED***James Gerard Stranch , IV**

Stranch, Jennings & Garvey, PLLC

223 Rosa L. Parks Avenue

Freedom Building

Ste 200

Nashville, TN 37203

615-254-8801

Fax: 615-250-3937

Email: gstranch@stranchlaw.com

*ATTORNEY TO BE NOTICED***Nathan J. Fink**

(See above for address)

*ATTORNEY TO BE NOTICED***Yana A. Hart**

(See above for address)

*ATTORNEY TO BE NOTICED***Erik Johnson**

(See above for address)

*ATTORNEY TO BE NOTICED***Plaintiff****Jane Doe***1-11, Consolidated from 25-10946*represented by **Beth M. Rivers**

Pitt McGehee Palmer & Rivers

117 W. Fourth Street

Suite 200

Royal Oak, MI 48067-3804

248-398-9800

Email: brivers@pittlawpc.com

*ATTORNEY TO BE NOTICED***Danielle Young Canepa**

Pitt McGehee Palmer Bonanni & Rivers PC

117 W. 4th Street

Suite 200

Royal Oak, MI 48067

248-398-9800

Email: dcanepa@pittlawpc.com

*ATTORNEY TO BE NOTICED***Jason J. Thompson**

Sommers Schwartz, P.C.

One Towne Square
Suite 1700
Southfield, MI 48076
248-355-0300
Fax: 248-436-8453
Email: jthompson@sommerspc.com
ATTORNEY TO BE NOTICED

Kevin Michael Carlson
Pitt McGehee Palmer & Rivers PC
117 West Fourth Street
Suite 200
Royal Oak, MI 48067
248-398-9800
Email: kcarlson@pittlawpc.com
ATTORNEY TO BE NOTICED

Lisa M. Esser
Sommers Schwartz, P.C.
One Towne Square
Ste 1700
Southfield, MI 48076
248-355-0300
Email: lesser@sommerspc.com
ATTORNEY TO BE NOTICED

Matthew G. Curtis
Sommers Schwartz, P.C.
One Towne Square
17th Floor
Southfield
Southfield, MI 48076
248-746-4038
Fax: 248-936-2124
Email: mcurtis@sommerspc.com
ATTORNEY TO BE NOTICED

Megan Bonanni
Pitt, McGehee,
117 W. Fourth Street
Suite 200
Royal Oak, MI 48067-3804
248-398-9800
Email: mbonanni@pittlawpc.com
ATTORNEY TO BE NOTICED

Richard L. Groffsky
Sommers Schwartz
One Towne Center
Ste 1700
Southfield, MI 48076
248-746-4028
Email: rgroffsky@sommerspc.com
ATTORNEY TO BE NOTICED

Sara Mickovic

Sommers Schwartz, P.C.

1 Towne Square

#1700

Southfield, MI 48076

248-916-2730

Email: smickovic@sommerspc.com

*ATTORNEY TO BE NOTICED***Yana A. Hart**

(See above for address)

*ATTORNEY TO BE NOTICED***Erik Johnson**

(See above for address)

*ATTORNEY TO BE NOTICED***Plaintiff****Jane Doe***1-3, Consolidated from 25-10988*represented by **Robert J. Lantzy**

Buckfire & Buckfire

29000 Inkster Road

Ste. 150

Southfield, MI 48034

248-569-4646

Email: robert@buckfirelaw.com

*ATTORNEY TO BE NOTICED***Yana A. Hart**

(See above for address)

*ATTORNEY TO BE NOTICED***Erik Johnson**

(See above for address)

*ATTORNEY TO BE NOTICED***Plaintiff****Student Doe***Consolidated from 25-10999*represented by **Gary M. Klinger**

Milberg Coleman Bryson Phillips Grossman

PLLC

227 W. Monroe Street

Suite 2100

Chicago, IL 60606

866-252-0878

Email: gklinger@milberg.com

*ATTORNEY TO BE NOTICED***James Joseph Pizzirusso**

Hausfeld LLP

1200 17th Street, NW

Suite 600

Washington, DC 20036

202-540-7200

Fax: 202-540-7201

Email: jpizzirusso@hausfeld.com

ATTORNEY TO BE NOTICED

Mariya Weekes

Milberg Coleman Bryson Phillips
Grossman, PLLC

201 Sevilla Avenue, 2nd Floor

Coral Gables, FL 33134

954-647-1866

Email: mweekes@milberg.com

ATTORNEY TO BE NOTICED

Steven M. Nathan

Hausfeld LLP

NYC

33 Whitehall Street

Ste 14th Floor

New York, NY 10004

646-357-1100

Fax: 212-202-4322

Email: snathan@hausfeld.com

ATTORNEY TO BE NOTICED

Yana A. Hart

(See above for address)

ATTORNEY TO BE NOTICED

Erik Johnson

(See above for address)

ATTORNEY TO BE NOTICED

V.

Defendant

Matthew Weiss

Defendant

Regents of the University of Michigan

represented by **Daniel B. Tukel**

Butzel Long

201 West Big Beaver Road

Suite 1200

Troy, MI 48084

313-225-7047

Email: tukel@butzel.com

ATTORNEY TO BE NOTICED

Sheldon H. Klein

Butzel

201 West Big Beaver Road

Suite 1200

Troy, MI 48084

248-258-1414

Fax: 248-258-1439

Email: klein@butzel.com
ATTORNEY TO BE NOTICED

Defendant**University of Michigan**

represented by **Daniel B. Tukel**
(See above for address)
ATTORNEY TO BE NOTICED

Sheldon H. Klein
(See above for address)
ATTORNEY TO BE NOTICED

Defendant**Keffer Development Services, LLC**

represented by **Carl Andrew Fejko**
Dillon McCandless King Coulter Graham
Civil Practice
128 West Cunningham St.
Butler, PA 16001
724-822-2148
Email: cfejko@dmkcg.com
ATTORNEY TO BE NOTICED

Jordan P. Shuber
Dillon McCandless King Coulter &
Graham, LLP
128 West Cunningham Street
Butler, PA 16001
724-283-2200
Fax: 724-283-2298
Email: jshuber@dmkcg.com
ATTORNEY TO BE NOTICED

Richard Shenkan
Shenkan Injury Lawyers, LLC
6550 Lakeshore Street
West Bloomfield, MI 48323
412-716-5800
Fax: 888-769-1774
Email: rshenkan@shenkanlaw.com
ATTORNEY TO BE NOTICED

Thomas W. King , III
Dillon McCandless King Coulter & Graham
LLP
128 West Cunningham Street
Buter, PA 16001
724-283-2200
Email: tking@dmkcg.com
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
------------	---	-------------

03/21/2025	1	COMPLAINT filed by All Plaintiffs against All Defendants with Jury Demand. Plaintiff requests summons issued. Receipt No: AMIEDC-10167469 - Fee: \$ 405. County of 1st Plaintiff: Washtenaw - County Where Action Arose: Washtenaw - County of 1st Defendant: Washtenaw. [Previously dismissed case: No] [Possible companion case(s): None] (Stinar, Parker) (Entered: 03/21/2025)
03/24/2025	2	SUMMONS Issued for *Keffer Development Services, LLC* (LHam) (Entered: 03/24/2025)
03/24/2025	3	SUMMONS Issued for *Regents of the University of Michigan* (LHam) (Entered: 03/24/2025)
03/24/2025	4	SUMMONS Issued for *University of Michigan* (LHam) (Entered: 03/24/2025)
03/24/2025	5	SUMMONS Issued for *Matthew Weiss* (LHam) (Entered: 03/24/2025)
03/24/2025		A United States Magistrate Judge of this Court is available to conduct all proceedings in this civil action in accordance with 28 U.S.C. 636c and FRCP 73. The Notice, Consent, and Reference of a Civil Action to a Magistrate Judge form is available for download at http://www.mied.uscourts.gov (LHam) (Entered: 03/24/2025)
03/24/2025	6	ORDER of RECUSAL and REASSIGNING CASE from District Judge Robert J. White to District Judge Mark A. Goldsmith. (SSch) (Entered: 03/24/2025)
03/24/2025	7	MOTION for Order to <i>Maintain Pseudonyms</i> by All Plaintiffs. (Stinar, Parker) (Entered: 03/24/2025)
03/27/2025	8	NOTICE of Appearance by John W Barrett on behalf of Jane Doe 1, Jane Doe 2. (Barrett, John) (Entered: 03/27/2025)
03/27/2025	9	NOTICE of Appearance by Bart Cohen on behalf of Jane Doe 1, Jane Doe 2. (Cohen, Bart) (Entered: 03/27/2025)
03/28/2025	10	NOTICE of Appearance by Daniel B. Tukel on behalf of Regents of the University of Michigan, University of Michigan. (Tukel, Daniel) (Entered: 03/28/2025)
03/28/2025	11	NOTICE of Appearance by D. Todd Mathews on behalf of Jane Doe 1, Jane Doe 2. (Mathews, D.) (Entered: 03/28/2025)
04/02/2025	12	STIPULATED ORDER EXTENDING TIME TO RESPOND TO COMPLAINT - (Response due by 6/2/2025) - Signed by District Judge Mark A. Goldsmith. (CCie) (Entered: 04/02/2025)
04/03/2025	13	CERTIFICATE of Service/Summons Returned Executed. Keffer Development Services, LLC served on 3/31/2025, answer due 4/21/2025. (Stinar, Parker) (Entered: 04/03/2025)
04/07/2025	14	STIPULATED ORDER REGARDING USE OF PSEUDONYMS AND RESOLVING PLAINTIFFS' MOTION TO MAINTAIN PSEUDONYMS (ECF NO. 7) - Signed by District Judge Mark A. Goldsmith. (CCie) (Entered: 04/07/2025)
04/08/2025	15	MOTION Motion Granted-Order Entered by All Plaintiffs. (Attachments: # 1 Index of Exhibits Index, # 2 Exhibit Exhibit A, # 3 Exhibit Exhibit B, # 4 Exhibit Exhibit C, # 5 Exhibit Exhibit D, # 6 Exhibit Exhibit E, # 7 Exhibit Exhibit F, # 8 Exhibit Exhibit G) (Stinar, Parker) Modified on 4/9/2025 (LHam).[DOCUMENT IS MOTION FOR EXPEDITED DISCOVERY] (Entered: 04/08/2025)
04/09/2025	16	ORDER OF RECUSAL AND REASSIGNING CASE from Magistrate Judge David R. Grand to Magistrate Judge Elizabeth A. Stafford. (NAhm) (Entered: 04/09/2025)

04/14/2025	17	NOTICE of Appearance by Benjamin Gillig on behalf of Jane Doe 1, Jane Doe 2. (Gillig, Benjamin) (Entered: 04/14/2025)
04/15/2025	18	NOTICE of Appearance by Sheldon H. Klein on behalf of Regents of the University of Michigan, University of Michigan. (Klein, Sheldon) (Entered: 04/15/2025)
04/15/2025	19	MOTION to Consolidate Cases and to Appoint Interim Lead Counsel by All Plaintiffs. (Attachments: # 1 Index of Exhibits, # 2 Exhibit) (Stinar, Parker) (Entered: 04/15/2025)
04/15/2025	20	NOTICE of Appearance by Katherine E. Charonko on behalf of All Plaintiffs. (Charonko, Katherine) (Entered: 04/15/2025)
04/15/2025	21	MOTION for Affirmative Injunctive Relief by All Plaintiffs. (Attachments: # 1 Index of Exhibits, # 2 Exhibit, # 3 Exhibit) (Stinar, Parker) (Entered: 04/15/2025)
04/16/2025	22	MOTION to Consolidate Cases <i>and To Convene Case Management Conference</i> by Regents of the University of Michigan, University of Michigan. (Tukel, Daniel) (Entered: 04/16/2025)
04/16/2025	23	NOTICE of Appearance by Bryce Thomas Hensley on behalf of All Plaintiffs. (Hensley, Bryce) (Entered: 04/16/2025)
04/16/2025	24	NOTICE of Appearance by Michael R. Grieco on behalf of All Plaintiffs. (Grieco, Michael) (Entered: 04/16/2025)
04/17/2025	25	NOTICE of Appearance by Brian A Glasser on behalf of All Plaintiffs. (Glasser, Brian) (Entered: 04/17/2025)
04/18/2025	26	NOTICE of Appearance by Aimee Wagstaff on behalf of Jane Doe 1, Jane Doe 2. (Wagstaff, Aimee) (Entered: 04/18/2025)
04/21/2025	27	NOTICE of Appearance by Richard Shenkan on behalf of Keffer Development Services, LLC. (Shenkan, Richard) (Entered: 04/21/2025)
04/22/2025	28	ORDER Regarding Status Conference. Signed by District Judge Mark A. Goldsmith. (HRya) (Entered: 04/22/2025)
04/22/2025	29	NOTICE TO APPEAR REMOTELY: Status Conference set for 5/14/2025 at 9:00 AM before District Judge Mark A. Goldsmith. (HRya) (Entered: 04/22/2025)
04/22/2025	30	STIPULATED ORDER Extending Time for Keffer Development Services, LLC to Respond to 1 Complaint. Response due by 6/2/2025. Signed by District Judge Mark A. Goldsmith. (HRya) (Entered: 04/22/2025)
04/22/2025	31	RESPONSE to 15 MOTION Motion Granted-Order Entered <i>Response in Opposition to Plaintiffs' Motion for Expedited Discovery</i> filed by Regents of the University of Michigan, University of Michigan. (Tukel, Daniel) (Entered: 04/22/2025)
04/23/2025	32	NOTICE by All Plaintiffs of <i>Filing Motion for Staus Conference</i> (Thompson, Jason) (Entered: 04/23/2025)
04/23/2025	33	MOTION to Stay <i>Response to Plaintiffs' Motion for Affirmative Injunctive Relief</i> by Regents of the University of Michigan, University of Michigan. (Tukel, Daniel) (Entered: 04/23/2025)
04/23/2025	34	MOTION Enter Order Appointing Marko Law PLLC and Hurwitz Law PLLC as Interim Lead Counsel by All Plaintiffs. (Marko, Jonathan) Modified on 4/23/2025 (JPar). [DOCUMENT IS A RESPONSE TO 19 PER ATTORNEY] (Entered: 04/23/2025)

04/24/2025	35	NOTICE of Appearance by David L. Selby, II on behalf of All Plaintiffs. (Selby, David) (Entered: 04/24/2025)
04/24/2025	36	Amended MOTION to Amend/Correct 19 MOTION to Consolidate Cases and to Appoint Interim Lead Counsel by All Plaintiffs. (Attachments: # 1 Index of Exhibits, # 2 Exhibit) (Stinar, Parker) (Entered: 04/24/2025)
04/25/2025	37	NOTICE of Appearance by Patrick C. Lannen on behalf of All Plaintiffs. (Lannen, Patrick) (Entered: 04/25/2025)
04/25/2025	38	NOTICE of Appearance by Erik Johnson on behalf of All Plaintiffs. (Johnson, Erik) (Entered: 04/25/2025)
04/29/2025	39	STIPULATED ORDER Extending Deadline Plaintiff's to File Reply to 15 MOTION for Expedited Discovery :(Reply due by 5/2/2025) Signed by District Judge Mark A. Goldsmith. (JOWe) (Entered: 04/29/2025)
04/30/2025	40	REPLY to Response re 19 MOTION to Consolidate Cases and to Appoint Interim Lead Counsel filed by All Plaintiffs. (Stinar, Parker) (Entered: 04/30/2025)
04/30/2025	41	NOTICE of Appearance by Thomas W. King, III on behalf of Keffer Development Services, LLC. (King, Thomas) (Entered: 04/30/2025)
04/30/2025	42	NOTICE of Joinder/Concurrence in 33 MOTION to Stay <i>Response to Plaintiffs' Motion for Affirmative Injunctive Relief</i> filed by University of Michigan, Regents of the University of Michigan by Keffer Development Services, LLC (King, Thomas) (Entered: 04/30/2025)
04/30/2025	43	RESPONSE to 22 MOTION to Consolidate Cases <i>and To Convene Case Management Conference</i> filed by All Plaintiffs. (Stinar, Parker) (Entered: 04/30/2025)
05/02/2025	44	REPLY to Response re 15 MOTION Motion Granted-Order Entered <i>Motion for Expedited Discovery</i> filed by All Plaintiffs. (Stinar, Parker) (Entered: 05/02/2025)
05/06/2025	45	NOTICE by All Plaintiffs re 32 Notice (Other) <i>Corrected Notice of Filing Motion for Status Conference</i> (Thompson, Jason) (Entered: 05/06/2025)
05/06/2025	46	RESPONSE to 21 MOTION for Affirmative Injunctive Relief filed by Regents of the University of Michigan, University of Michigan. (Attachments: # 1 Index of Exhibits, # 2 Exhibit A, Peoples v. Michigan Department of Corrections, # 3 Exhibit B, Solomon v. Shoulders, # 4 Exhibit C, Yeisley v. University of Iowa Hospitals and Clinics, # 5 Exhibit D, Stephenson v. University of Michigan) (Tukel, Daniel) (Entered: 05/06/2025)
05/06/2025	47	NOTICE of Joinder/Concurrence in 46 Response to Motion, filed by University of Michigan, Regents of the University of Michigan by Keffer Development Services, LLC (King, Thomas) (Entered: 05/06/2025)
05/07/2025	48	RESPONSE to 33 MOTION to Stay <i>Response to Plaintiffs' Motion for Affirmative Injunctive Relief</i> filed by All Plaintiffs. (Stinar, Parker) (Entered: 05/07/2025)
05/07/2025	49	REPLY to Response re 21 MOTION for Affirmative Injunctive Relief filed by All Plaintiffs. (Stinar, Parker) (Entered: 05/07/2025)
05/09/2025	50	STATEMENT of Resolved and Unresolved Issues <i>Joint</i> by All Plaintiffs (Stinar, Parker) (Entered: 05/09/2025)
05/09/2025	51	MOTION Plaintiff Counsels' Motion for Appointment of Interim Class Counsel by All Plaintiffs. (Attachments: # 1 Index of Exhibits, # 2 Exhibit A - Sommers Schwartz Attorney Bios, # 3 Exhibit B - Pitt McGehee Attorney Bios, # 4 Exhibit C - Clarkson Firm Attorney Bios, # 5 Exhibit D - Marko Firm Attorney Bio, # 6 Exhibit E - Weiss Indictment, # 7 Exhibit F - Illinois Complaint, # 8 Exhibit G - Ohio Complaint, # 9 Exhibit H -

		Massachusetts Complaint, # 10 Exhibit I - North Carolina Complaint, # 11 Exhibit J - California Complaint, # 12 Exhibit K - Michigan Court of Claims Complaint, # 13 Exhibit L - Midland Dam Case Order re Liaison Counsel) (Thompson, Jason) (Entered: 05/09/2025)
05/14/2025		Minute Entry for remote proceedings before District Judge Mark A. Goldsmith: Status Conference held on 5/14/2025. (Court Reporter: None Present, Not on the Record) (JHea) (Entered: 05/14/2025)
05/14/2025	52	NOTICE of Appearance by Carl Andrew Fejko on behalf of Keffer Development Services, LLC. (Fejko, Carl) (Entered: 05/14/2025)
05/14/2025	53	CERTIFICATE OF SERVICE by All Plaintiffs of <i>Summons & Complaint</i> (Stinar, Parker) (Entered: 05/14/2025)
05/15/2025	54	NOTICE of Appearance by Jordan P. Shuber on behalf of Keffer Development Services, LLC. (Shuber, Jordan) (Entered: 05/15/2025)
05/16/2025	55	RESPONSE to 51 MOTION Plaintiff Counsels' Motion for Appointment of Interim Class Counsel filed by All Plaintiffs. (Stinar, Parker) (Entered: 05/16/2025)
05/16/2025	56	SUPPLEMENTAL BRIEF re 51 MOTION Plaintiff Counsels' Motion for Appointment of Interim Class Counsel filed by Jane Doe 1, Jane Doe 2. (Hart, Yana) (Entered: 05/16/2025)
05/20/2025	57	REPLY to Response re 21 MOTION for Affirmative Injunctive Relief filed by All Plaintiffs. (Attachments: # 1 Exhibit) (Stinar, Parker) (Entered: 05/20/2025)
05/23/2025	58	ORDER FOR CONSOLIDATION AND RELATED MATTERS. Signed by District Judge Mark A. Goldsmith. (JHea) (Entered: 05/23/2025)
05/23/2025	59	Notice to Parties Regarding Consolidated Case: Order of consolidation entered on *5/23/2025*. Designated lead case number is *25-10806*. (JHea) (Entered: 05/23/2025)
06/03/2025	60	REQUEST FOR CLERK'S ENTRY OF DEFAULT as to Matthew Weiss by All Plaintiffs. (Johnson, Erik) (Entered: 06/03/2025)
06/03/2025	61	STIPULATED ORDER EXTENDING DEADLINE TO FILE CONSOLIDATED COMPLAINT. Consolidated Complaint due by 6/20/2025, Responsive Pleadings due by 8/8/2025. Signed by District Judge Mark A. Goldsmith. (JHea) (Entered: 06/03/2025)
06/04/2025	62	NOTICE TO APPEAR REMOTELY VIA ZOOM: Attorney Only Status Conference set for 6/12/2025 12:00 PM before District Judge Mark A. Goldsmith. (JHea) (Entered: 06/04/2025)
06/04/2025	63	NOTICE of Appearance by Mariya Weekes on behalf of Student Doe. (Weekes, Mariya) (Entered: 06/04/2025)
06/05/2025	64	CLERK'S ENTRY OF DEFAULT as to *Matthew Weiss* (JBro) (Entered: 06/05/2025)

PACER Service Center			
Transaction Receipt			
06/05/2025 16:07:13			
PACER Login:	ThomaKingtking	Client Code:	
Description:	Docket Report	Search Criteria:	2:25-cv-10806-MAG-EAS

Billable Pages:	14	Cost:	1.40
--------------------	----	-------	------

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

JANE DOE 1, and JANE DOE 2,
Plaintiffs,

vs.

MATTHEW WEISS; the REGENTS
OF THE UNIVERSITY OF
MICHIGAN; the UNIVERSITY OF
MICHIGAN; KEFFER
DEVELOPMENT SERVICES, LLC,

Defendants.

Case No. ____

Hon. _____

Mag. _____

Jury Trial Demanded

PLAINTIFFS' CLASS ACTION COMPLAINT AND JURY DEMAND

RECORDS PRESERVATION NOTICE

Defendants are hereby notified to preserve during the pendency of this action all records and documents in all forms and formats relating to this case and to notify employees, agents, and contractors that they are required to take appropriate action to do the same.

Plaintiffs, JANE DOE 1 and JANE DOE 2 (“Plaintiffs”), through their attorneys, Stinar Gould Grieco & Hensley, for their Complaint against MATTHEW WEISS, the REGENTS OF THE UNIVERSITY OF MICHIGAN, the UNIVERSITY OF MICHIGAN, and KEFFER DEVELOPMENT SERVICES, LLC, states as follows:

THE PARTIES, JURISDICTION, AND VENUE

1. Plaintiff Jane Doe 1 was a student athlete at the University of Michigan between 2017 and 2018 and was a member of the Michigan Women’s Gymnastics team.

2. Plaintiff Jane Doe 1 is domiciled in Washtenaw County, Michigan, in the city of Ypsilanti.

3. Plaintiff Jane Doe 2 was a student athlete at the University of Michigan between 2017 and 2023 and was a member of the Michigan Women’s Soccer team.

4. Plaintiff Jane Doe 2 is domiciled in Oakland County, Michigan, in the City of Northville.

5. The Regents of the University of Michigan (the “Regents”) is a body corporate, with the right to be sued, vested with the government of the university. Mich. Comp. Laws § 390.3 and § 390.4.

6. The University of Michigan (the “University”) is a public university organized and existing under the laws of the State of Michigan.

7. The University received and receives state financial assistance and is therefore, among other reasons, subject to the laws of the State of Michigan.

8. Keffer Development Services, LLC (“Keffer”) is a Pennsylvania limited liability company that has continuously and systematically done business in the State of Michigan through its direct providing of services to residents and entities within the State of Michigan for which it has been handsomely compensated and has therefore purposefully availed itself of protections of the laws of the State of Michigan.

9. Keffer’s misconduct and legal failures as detailed in this Complaint occurred specifically with respect to Plaintiffs who reside in Michigan and while Plaintiffs resided in Michigan.

10. Matthew Weiss is an individual who resides in Michigan.

11. Jurisdiction is proper in this Court under 28 U.S.C. §§ 1331 and 1367 because this matter involves a cause of action under the Stored Communications Act, 18 U.S.C. § 2701(a) *et seq.* and the court has supplemental jurisdiction of the other causes of action under 28 U.S.C. §1367(a).

12. Venue is appropriate in this district under 28 U.S.C. §1391 because a substantial part of the events or omissions giving rise to these claims occurred in this district and Defendants are subject to personal jurisdiction in this district.

COMMON ALLEGATIONS

13. Weiss was employed by the University.

14. Weiss's actions were in furtherance of his job duties for the University.

15. The Regents are responsible and had a duty to ensure that the University runs itself with integrity and care for the students.

16. It breached that duty by failing to supervise and monitor Weiss and as a result Plaintiffs and thousands of others have had their privacy illegally invaded.

17. The Regents are also responsible for overseeing the University's operations, finances, and policy, including approving budgets, tuition rates, and construction projects.

18. The Regents also failed in that duty by failing to consider, implement, or follow a policy to oversee how or whether the University conducted its operations in a manner that would have in any manner monitored, supervised, and ensured that retention and employment of Weiss would not result in a breach of the privacy Plaintiffs entrusted to the University.

19. The Regents also failed in that duty by failing to take any action much less consider means by which to prevent the harm caused to Plaintiffs and their peers as alleged in this Complaint.

20. The Regents were supposed, but failed, to establish University policy, including to monitor personnel, including but not limited to Weiss, so that students on the campus were protected from their privacy being invaded.

21. The Regents were required but failed to ensure that the University offered services such as to have student athletes able to be treated by athletic professionals who do not invade their privacy.

22. The Regents recklessly failed to ensure media and information of and pertaining to student athletes including but not limited to Plaintiffs was safely provided since Plaintiffs and other similar to them entrusted the Regents to do so.

23. The Regents had an obligation to support Plaintiffs, and to develop the campus, its operations including student services, and admissions, and financial aid, among others, in a way that at least considered having and executing security measures to protect the personal, private, and intimate images and information of the Plaintiffs and others similar to them.

24. The Regents breached those duties because they failed to consider or implement any security measures to protect the personal, private, and intimate images and information of the Plaintiffs and others similar to them.

25. The Regents were responsible for financial oversight of the University but failed to prudently exercise that duty because they placed avoiding cost of learning, having, and implementing security measures to protect the personal,

private, and intimate images and information of the Plaintiffs and others similar to them, as more important than incurring the cost of establishing and paying for programs to so implement safety policies, and to monitor and ensure student safety.

26. The Regents are supposed to regulate all three U-M campuses but failed to do so by failing to consider or implement any policies to review, discover, or prevent the willful invasions of privacy committed by Weiss as a result of the access the University provided to him to so invade the privacy of the student athletes including but not limited to Plaintiffs who entrusted themselves to the University and the Regents.

27. The University itself had all of the same duties as the Regents.

28. The University itself breached all of the same duties and in the same and/or similar manners as the Regents.

29. The Plaintiffs and others like them entrusted the University to safeguard their bodily images and information.

30. The University breached the heightened duty it had and recklessly permitted Weiss to invade the Plaintiffs' privacy and likewise for their student athlete peers and expose them and their intimate images.

31. The Regents also had and breached general supervision privileges and obligations to "control" and "direct" all expenditures of funds but failed to ensure any of the many millions of public dollars given to the University were used to study,

select, and implement safety measures to protect student athletes' private and personal body images and information, particularly female athletes, while at the same time spending tens if not hundreds of millions of dollars on other expenses that are wholly ignorant of student athlete health, safety, and privacy.

32. The University employed Weiss.

33. The University controlled Weiss.

34. The University assigned and directed job duties to and upon Weiss.

35. Those job duties and direction directly resulted in Weiss accessing private, personal, intimate images and information of Plaintiffs and others similar to them, all of which were private, and entrusted to be safeguarded by the university and its agents.

36. The University took no action to monitor Weiss despite providing him with the ability and means to invade Plaintiffs' privacy and the privacy of others.

37. The University breached the confidences that Plaintiffs and others similar to Plaintiffs entrusted to the University and did so by providing Weiss with the electronic credentials and ability to track and spy on students athletes including Plaintiffs, and to use those credentials to invade Plaintiffs' private lives and obtain and use images of them and personal information relating to them.

38. With no University supervision, and during execution of his official duties as an employee of the University, Weiss invaded Plaintiffs' privacy and the privacy of others in similar postures.

39. The misconduct, recklessness, and bad acts of the Regents, the University, and Weiss also included and involved Keffer.

40. Keffer's misconduct, negligence, and recklessness also contributed to Weiss invading the privacy of Plaintiffs and their fellow student athletes.

41. Keffer agreed to safely maintain and store information, images, expressions, and videos of Plaintiffs and their peers in secure manner, free from access from employees of the University such as Weiss or third parties.

42. Keffer knew that the images and information of Plaintiffs and others similar to them would be personal, private, and intimate.

43. Keffer knowingly and intentionally took on the obligation to safeguard and protect the personal, private, and intimate images and information entrusted to Keffer by Plaintiffs and others similar to them.

44. Keffer breached those obligations by failing to consider, enact, or implement any policy, procedure, or security measure to safeguard and protect the personal, private, and intimate images and information entrusted to Keffer by Plaintiffs and others similar to them.

45. Weiss accessed the personal, private, and intimate images and information entrusted to Keffer by Plaintiffs and others similar to them as a result of Keffer's failures to consider, enact, or implement any measure of security or protection.

46. Keffer collects information including private information about students and student athletes.

47. The University and the Regents authorized Keffer's collection of that information that is and was personal and private in nature.

48. Plaintiffs and others similar to them entrusted that the Regents and the University's authorization to and entrustment to Keffer would keep them safe and their private images and information private.

49. The Regents and the University failed to take any action to ensure that Keffer retained the privacy of the images and information of Plaintiffs and others like them.

50. The Regents' failures in this respect harmed Plaintiffs.

51. The University's failures in this respect harmed Plaintiffs.

52. Keffer failed to take any action to ensure that it retained the privacy of the images and information of Plaintiffs and others like them entrusted to Keffer.

53. Keffer failed to consider or take any action to protect against the access by Weiss of the private information, images, expressions, and videos of Plaintiffs and their peers.

54. Due to the negligent and reckless conduct of Keffer, the Regents, and the University (collectively, the “Non-Individual Defendants”), Weiss was able to, among other misconduct, invade the privacy of various individuals including but not limited to Plaintiffs and their peers.

55. Between approximately 2015 and January 2023, as alleged in the Indictment against him, Weiss gained access—without and in excess of authorization—to the social media, email, and/or cloud storage accounts of more than 3,300 people including but not limited to University student athletes, past and present, and including but not limited to Plaintiffs.

56. His ability to do so was aided by the University and the Regents both of whom permitted him to have access and use of electronic credentials that were means of viewing and downloading personal, private, and intimate images of Plaintiffs and others similar to them.

57. The Non-Individual Defendants failed to review Weiss’s activity, failed to supervise his activity, failed to review his retention in a prudent manner, and failed to ensure his work duties were being undertaken and completed with respect for Plaintiffs’ privacy and the privacy of others.

58. The Non-Individual Defendants failed to consider or implement any measure of security that provided protection for the privacy of information about student athletes including by failing to consider or have multiple authentication credentials, background checks, peer reviews, or oversight.

59. These failures allowed Weiss to access private, intimate, personal information pertaining to Plaintiffs and their peers, all of which was maintained by Keffer, as encouraged and authorized by the University and the Regents, and all of which Plaintiffs and other similar to them entrusted to the Non-Individual Defendants.

60. The recklessness and negligence and misconduct of the Regents, the University, and Keffer in these respects enabled Weiss to target female college athletes to obtain their private and sensitive information without authorization, including but not limited to Plaintiffs.

61. The Non-Individual Defendants knew that Weiss by virtue of his job duties would be at an advantage over others and would be able to access the other private information and privacy interests of the Plaintiffs and their peers.

62. Because the Regents, the University, and Keffer failed to undertake any reasonable security measures or background checks of Weiss, he was enabled to brazenly research and target and invade the privacy of various University athletes,

particularly female athletes, nearly all if not all such women were targeted based on their school affiliation, athletic history, and physical characteristics.

63. Because the Regents, the University, and Keffer failed to supervise Weiss, review his conduct, review his credentials, review his work, and left him free to prey on Plaintiffs and others, all without reporting what he was doing in furtherance of his duties, Weiss was able to execute his goal of obtaining private photographs and videos of Plaintiffs and others that were never intended to be shared beyond Plaintiffs' intimate partners, and likewise for other victims situated similar to the Plaintiffs.

64. As a result of the University's recklessness, the recklessness of the Regents, and the gross negligence of Keffer, Weiss downloaded personal, intimate digital photographs and videos of Plaintiffs and others, all of which Plaintiffs and other class members entrusted to the Non-Individual Defendants.

65. Because the Non-Individual Defendants negligently and recklessly failed to exercise any control over Weiss, Weiss, in furtherance of performance of his job duties, was able to successfully target athletes such as Plaintiffs and others similar to them and download, obtain, and use their private information, images, and videos.

66. Because the Non-Individual Defendants negligently and recklessly failed to keep tabs on Weiss, he was able to keep notes on individuals whose

photographs and videos he wanted, all of which he obtained, and then viewed, and the Non-Individual Defendants' failure to take any reasonable protective measures was so severe that Weiss even kept detailed notes commenting on the bodies and sexual preferences of Plaintiffs and their peers.

67. The information that the Non-Individual Defendants permitted Weiss to obtain is highly private, secretive, embarrassing when shared without authorization, and humiliating to become public without authorization.

68. Weiss obtained access—without and in excess of authorization—to student athlete databases of more than 100 colleges and universities across the country that were maintained by Keffer including but not limited to those of university athletes like Plaintiffs because the University and the Regents failed to take any action or even consider the harm Weiss could do, and actually did, as did Keffer.

69. Hundreds if not thousands of students still face harm because, despite notice from decades of athlete department complaints and abuse, and widely known social media stockpiles of information that beg for safekeeping, Keffer, the Regents and the University have failed again and again to undertake any review of how Plaintiffs' private and personal information is stored, maintained, and who can access such information, and from where.

70. The University and the Regents also failed to investigate Keffer, Keffer's protocols, and failed to monitor or establish safeguards for Keffer's work with the students and their private images to ensure they carried out their duties to safeguard and protect the private information entrusted to them.

71. The University and the Regents have also failed to consider or implement ways to prevent exposing students to Weiss.

72. Neither the University nor the Regents have explained or justified why they failed to undertake any review of the contract with Keffer, failed to investigate Keffer, failed to monitor or establish safeguards for Keffer's work with the students and their private images, and otherwise considered what action they should take to not expose students to Weiss.

73. Weiss, through the lack of control and enabling from the Non-Individual Defendants, obtained access to databases containing highly sensitive and private information of the Plaintiffs and others similar to them.

74. Many if not all of those databases are maintained by Keffer and was entrusted by Plaintiffs to be safeguarded.

75. Plaintiffs entrusted the University and the Regents to ensure Keffer safeguarded their private information and images.

76. All of the Non-Individual Defendants failed to consider or execute any action that would have been prudent and would have protected Plaintiffs' private

information and the private information of others in similar positions from being accessed by Weiss.

77. After gaining access to unsecured databases, Weiss downloaded the personally identifiable information (PII) and medical data of more than 150,000 athletes including Plaintiffs.

78. Weiss also downloaded passwords that athletes used to access Keffer's computer system to view and update the athletes' data, including that of Plaintiffs.

79. The athletes' passwords that Weiss downloaded were encrypted, but was poorly encrypted because of recklessness of the Non-Individual Defendants that Weiss while not being monitored or supervised by the Non-Individual Defendants cracked the encryption, assisted by basic research that he did on the internet.

80. Through open-source Weiss conducted additional research on targeted athletes such as Plaintiffs and obtained personal information such as their mothers' maiden names, pets, places of birth, and nicknames, all of which they had entrusted to Non-Individual Defendants to keep private and none of which the Non-Individual Defendants actually safeguarded in any reasonable manner.

81. Using the combined information that he obtained from the student athlete databases and his internet research, based on the lack of supervision or monitoring by the Non-Individual Defendants, despite their control over him, Weiss was able to obtain access to the social media, email, and/or cloud storage

accounts of more than 2,000 targeted athletes by guessing or resetting their passwords including but not limited to Plaintiffs.

82. Once he obtained access to the accounts of targeted athletes, Weiss searched for and downloaded personal, intimate photographs and videos that were not publicly shared, including but not limited to Plaintiffs and others similar to them.

83. Weiss also obtained access—without authorization—to the social media, email, and/or cloud storage accounts of more than 1,300 additional students and/or alumni from universities and colleges from around the country including but not limited to Plaintiffs, caused by the reckless disregard for the safety and personal privacy of the victims committed by the Non-Individual Defendants.

84. Once Weiss gained access to the accounts, he would search for and download personal, intimate photographs and videos.

85. The Regents took no reasonable actions to prevent this unauthorized access.

86. The University took no reasonable actions to prevent this unauthorized access.

87. Keffer took no reasonable actions to prevent this unauthorized access.

88. The Regents have taken no action to remedy the various tortious harms and invasions they permitted to occur.

89. The University has taken no action to remedy the various tortious harms and invasions they permitted to occur.

90. Keffer has taken no action to remedy the various tortious harms and invasions they permitted to occur.

91. In several instances, Weiss exploited vulnerabilities in the Non-Individuals' account authentication processes to gain access to the accounts of students or alumni including but not limited to Plaintiffs.

92. Weiss leveraged his access to these accounts to gain access to other social media, email, and/or cloud storage accounts.

93. The Regents took no action to prevent this unauthorized access.

94. The University took no action to prevent this unauthorized access.

95. Keffer took no action to prevent this unauthorized access.

96. The Non-Individual Defendants have long been on notice, and it is obvious, that the kind of information Weiss accessed would be reasonably expected to be kept private, would be embarrassing if accessed by third parties, and is the kind of data that in the modern world every commercial and governmental actor is expected to take action to safeguard, particularly since the young student athletes who are dedicated to the University and the Regents entrusted them to keep all such

private information and images confidential and free from access by third parties such as Weiss.

97. Despite all such notice and prior instances of breach of trust, the Non-Individual Defendants failed to protect Plaintiffs' private information and images, or to study, consider, or undertake any reasonable method to protect the Plaintiffs' privacy and the privacy of others.

98. From in and around 2015, to in and around January 2023, Weiss intentionally accessed—without authorization—information, images, and personal private information of Plaintiffs and others, including servers from identified and unidentified social media, email, and/or cloud storage providers that the Non-Individual Defendants knew Plaintiffs and others expected and entrusted them to protect and that they failed to protect.

99. Weiss obtained digital photographs, videos, and other private information belonging to more than 3,300 individuals including but not limited to Plaintiffs in furtherance of his job duties and his misconduct and the misconduct of the Non-Individual Defendants were violations of the Michigan and Maryland state torts of Invasion of Privacy.

100. From in and around May 2021, to in and around January 2023, Weiss, as a result of the reckless lack of protection, monitoring, or supervision from the

Non-Individual Defendants, knowingly transferred, possessed and used, without lawful authority, information, images, and pictures of Plaintiffs and others.

101. From in and around January 2020, to in and around October of 2021, Weiss intentionally accessed—as a result of the Non-Individual Defendants’ failure to protect the privacy of Plaintiffs and others—computers, networks, and information relating to Plaintiffs and others that was private in nature.

102. After compromising the passwords of approximately 150 accounts and gaining access to these same accounts because he was unsupervised or monitored, Weiss downloaded personally identifiable information (**PII**) and other health protected information and medical data of more than 150,000 athletes in furtherance of his job duties, including but not limited to Plaintiffs, all in violation of the Maryland, Michigan, and Pennsylvania state torts of Invasion of Privacy.

103. Weiss intended to and did obtain information that furthered his ability to reset the passwords for and access—without authorization—of social media, email, and/or cloud storage accounts of individuals like Plaintiffs whose information he obtained from Keffer’s systems, all of which were significantly more easily obtained because of the lack of oversight and monitoring from the Non-Individual Defendants, despite notice of the threat therefor.

104. From in and around October 2022, to in and around January 2023, Weiss intentionally—without and in excess of authorization—accessed servers Keffer operated, because the Non-Individual Defendants failed to supervise or monitor him, and he as a result obtained digital photographs, videos, and other private information of Plaintiffs and others, all in furtherance of job duties, including violations of the Michigan state tort of Invasion of Privacy.

105. From in and around December 21, 2022, to in and around December 23, 2022, Weiss intentionally accessed—without authorization—computers and servers of the University and the Regents and their technology service providers, thereby invading the privacy of Plaintiffs and others, from and after the Non-Individual Defendants’ failure to monitor or supervise Weiss, despite the trust that the Plaintiffs placed in the University and the Regents.

106. As additional damage, and as a result of the Non-Individual Defendants’ failure to monitor or supervise Weiss, Weiss was able to reset various passwords including Plaintiffs’ account, which amounts to various tortious acts, including violations of privacy, and was perpetrated through various social media, email, and/or cloud storage accounts of one or more University alumni.

107. Plaintiffs have incurred significant monetary and nonmonetary damages as a result of Defendants’ actions, inactions, torts, negligence, recklessness,

and misconduct, and have been so damaged in excess of \$75,000, exclusive of costs, interest, and fees.

CLASS ALLEGATIONS

108. Plaintiffs brings this lawsuit individually and as a class action on behalf of all others similarly situated pursuant to Rule 23.

109. This action satisfies the numerosity, commonality, predominance, typicality and adequacy of the rule.

110. The Class is currently defined as:

All persons whose personal information, images, data, social media, or videos were access by Weiss without authorization (the “Class Members”).

111. Numerosity: Although the exact number of Class Members is uncertain at this time and can only be ascertained through forthcoming appropriate discovery, the number is great enough such that joinder is impracticable and is estimated to exceed one thousand members (1,000).

112. Law enforcement officials have disclosed the numbers of victims is a great many and numerosity is established.

113. The disposition of the claims of these Class Members in a single action will provide substantial benefits to all parties and to the Court, and preserve resources, avoid potentially inconsistent results, and be an equitable and efficient manner to adjudicate the claims.

114. The Class Members are readily identifiable from information and records in the possession of the federal and state authorities, the Regents, the University, and Keffer.

115. The electronic records possessed by the Non-Individual Defendants who conducted their own investigation can confirm the identification of class membership.

116. Commonality: The facts and proofs that show how, where, who, when, and through what mediums the invasions of Plaintiffs occurred and as occurred to the other Class Members are best and fairly determined in one stroke.

117. The actions, inactions, negligence, and recklessness of the Non-Individual Defendants is common as to all Plaintiffs and Class Members.

118. The downloads and invasions by Weiss and the improper conduct accessing private information through unsecure facilities without permission is common to all Class Members and has caused injury to the Plaintiffs and Class Members in virtually identical manners.

119. The vast majority of the factual proofs and questions of law common to the Plaintiffs and to the Class Members predominate over any individual questions.

120. Plaintiffs claims are typical of the Class Members because they are highly similar and the same and related in time, space, and origin.

121. Plaintiffs are more than adequate representatives of the class because they are motivated to seek justice, and adequately represent the harms perpetrated upon the class.

122. Maintaining this action as a class action is superior to other methods of adjudication, promoting the convenient administration of justice because:

- a. The pursuit of separate actions by individual Class Members would risk inconsistent or varying adjudications that would confront Defendants with potentially incompatible standards of conduct;
- b. Many victims will not come forward without a certified class.
- c. Final equitable relief will be appropriate with respect to the Class as a whole for any monitoring, protection, therapy and other equitable forms of relief that may be provided;
- d. This action is manageable as a class action and would be unmanageable any other way;
- e. Absent the class action, individual Class Members may not know if they have been recorded; where such images are currently being stored or are accessible by others; and their injuries are likely to go unaddressed and unremedied; and,
- f. Individual Class Members may not have a significant interest in controlling the prosecution of separate actions.

**COUNT I – VIOLATION OF THE COMPUTER FRAUD
AND ABUSE ACT – 18 U.S.C. § 1030**

123. Plaintiffs incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

124. Weiss violated the Computer Fraud and Abuse Act by accessing without authorization Plaintiffs’ private information.

125. Weiss did so in connection with his job duties given to him by the University.

126. Weiss violated the Act because he “intentionally accesse[d] a computer without authorization” and/or “exceed[ed] authorized access, and thereby obtain[ed] ... information.” 18 U.S.C. § 1030(a)(2)(C).

127. Under the law, Weiss was an “inside hacker” because he accessed a computer with permission that dealt with Plaintiffs and the Class Members as student athletes, however, Weiss in connection with and furtherance of his job duties then exceeded the parameters of authorized access by entering an area of computerized network of information that was off-limits.

128. As the law has described the situation, it would be like opening your office door and, to your surprise, find someone already inside. If the person is a stranger with no right to be in the building, they lack authorization. If the person is a coworker from down the hall, they may have exceeded their authorized access

129. Weiss's violations were intentional because he knew he was unauthorized and proceeded nevertheless and did so with approval from the University.

130. The University is vicariously liable for his actions because he did so in furtherance of his role as a medical sports employee of the University's athletic department.

131. The law is clear that the University is vicariously liable for any completed offenses of its agents.

132. Under 18 U.S.C. § 1030(g), Plaintiffs may recover damages in this civil action from Weiss and the University along with injunctive relief or other equitable relief.

133. Plaintiffs should be awarded all such forms of damages in this case for Weiss's and the University's willful violation that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

COUNT II – VIOLATIONS OF STORED COMMUNICATIONS ACT

134. Plaintiffs incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

135. The Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, prohibits the intentional access of web-based cloud storage and media accounts such as those at issue and other accounts hosted by Keffer that did and do, like for Plaintiffs,

contain personal, private, and intimate information about and relating to Plaintiffs and others situated similar to Plaintiffs.

136. Specifically, 18 U.S.C. § 2701(a) states that anyone who:

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

137. Plaintiffs' electronic information and communications were in electronic storage and fit directly within the protections of the statute.

138. The information, messages, files, and media were accessed by Weiss without authorization, in connection with his job duties performed for the University.

139. Weiss's access without authorization in connection with his University job duties was intentional and knowingly done.

140. There is no manner in which Plaintiffs' private information, messages, files, and media that is in issue could have been obtained without unauthorized access and would not have been obtained without unauthorized access had Weiss not been an employee of the University working in the specific sports medicine capacity for which the University hired and employed him.

141. Section 2707 of the Stored Communications Act states that a party may bring a civil action for the violation of this statute.

142. It is a strict liability statute.

143. The statute provides that a person aggrieved by a violation of the act may seek appropriate relief including equitable and declaratory relief, actual damages or damages no less than \$1,000, punitive damages, and reasonable attorney's fee[s] and other litigation costs reasonably incurred according to 18 U.S.C. § 2707(b)-(c).

144. The University's and Weiss's access to Plaintiffs' private, personal, and intimate information, messages, files, and media was in violation of 18 U.S.C. § 2701(a).

145. The University and Weiss knew they did not have authority to access Plaintiffs' private, personal, and intimate information, messages, files, and media and accessed it nevertheless.

146. That willful misconduct violated the Stored Communications Act on various occasions.

147. Plaintiffs have incurred significant monetary and nonmonetary damages as a result of these violations of the Stored Communications Act, and Plaintiffs request to be compensated for their injuries.

148. Under the statute, Plaintiffs should be granted the greater of (1) the sum of their actual damages suffered and any profits made by the University and Weiss as a result of the violations or (2) \$1,000 per violation of the Stored Communications Act.

149. Since the violations were willful, the Court should assess punitive damages against Defendants in addition.

150. Plaintiffs should be granted reasonable attorney fees and costs as well.

COUNT III – VIOLATION OF TITLE IX, 20 U.S.C. § 1681(A) *Et Seq.*

151. Plaintiffs incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

152. Title IX's provides, "No person in the United States shall on the basis of sex, be ... subject to discrimination under any education program or activity receiving Federal financial assistance ..."

153. Plaintiffs are each a "person" under the Title IX statutory language.

154. Weiss targeted women in his unwanted invasions of privacy and his misconduct is discrimination on the basis of sex.

155. The University receives federal financial assistance for its education program and is therefore subject to the provisions of Title IX of the Education Act of 1972, 20 U.S.C. § 1681(a), *et seq.*

156. The University is required under Title IX to investigate allegations of sexual harassment.

157. The University was aware of the sensitive nature of the private and personal information of Plaintiffs to which Weiss was able to access given his role.

158. The University and Regents acted with deliberate indifference to sexual harassment by:

- a. Failing to protect Plaintiffs and others as required by Title IX;
- b. Failing to adequately investigate and address the complaints regarding the deeply sensitive information Plaintiffs provided;
- c. Failing to institute corrective measures to prevent Weiss from sexually harassing other students; and
- d. Failing to adequately investigate the other multiple acts of deliberate indifference.

159. The University and the Regents acted with deliberate indifference as their lack of response to the sexual harassment was clearly unreasonable in light of the known circumstances.

160. The University's failure to promptly and appropriately protect, investigate, and remedy and respond to the sexual harassment of women has effectively denied them equal educational opportunities at the University, including medical care and sports training.

161. At the time the Plaintiffs received some medical training services from the University, they did not know the Non-Individual Defendants failed to adequately consider their safety including in their engagement, hire, training, and supervision of Weiss.

162. As a result of the University's and the Regents' deliberate indifference, Plaintiffs have suffered loss of educational opportunities and/or benefits.

163. Plaintiffs have and incurred, and will continue to incur, attorney's fees and costs of litigation.

164. At the time of Defendants' misconduct and wrongful actions and inactions, Plaintiffs were unaware, and or with reasonable diligence could not have been aware, of Defendants' institutional failings with respect to their responsibilities under Title IX.

165. The Regents and the University maintained a policy and/or practice of deliberate indifference to protection of female student athletes.

166. Defendants' policy and/or practice of deliberate indifference to protection against the invasion of privacy for female athletes created a heightened risk of sexual harassment.

167. Defendants had the ability to prevent the privacy invasion and sexual harassment failed to so prevent the invasions and harassment.

168. Because of the Regents' and the University's policy and/or practice of deliberate indifference, Plaintiffs had their privacy invaded and were sexually harassed by Weiss.

169. Plaintiffs should be awarded all such forms of damages in this case for Regents' and the University's conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

**COUNT IV -- VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C. § 1983 –
STATE CREATED DANGER**

170. Plaintiffs incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

171. The due process clause of the 14th Amendment provides that the state may not deprive a person of life, liberty or property without due process of law.

172. The Regents and the University recklessly exposed Plaintiffs to a dangerous predator, Weiss, knowing he could cause serious damage by sexually harassing female students, and also by violating their rights to privacy.

173. Plaintiffs as female student athletes were foreseeable victims.

174. The invasion of Plaintiffs' privacy was foreseeable.

175. The decisions and actions to deprive Plaintiff of a safe campus constituted affirmative acts that caused and/or increased the risk of harm, as well as physical and emotional injury, to Plaintiffs.

176. The University and the Regents acted in willful disregard for the safety of Plaintiffs.

177. The decisions and actions to deprive Plaintiffs a safe campus constituted affirmative acts that caused and/or increased the risk of harm, as well as physical and emotional injury, to Plaintiffs.

178. The University and the Regents acted in willful disregard for the safety of Plaintiffs.

179. Plaintiffs should be awarded all such forms of damages in this case for Regents' and the University's conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

COUNT V – FAILURE TO TRAIN AND SUPERVISE 42 U.S.C. § 1983

180. Plaintiffs incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

181. The University and the Regents had the ultimate responsibility and authority to train and supervise their employees, agents, and/or representatives including Weiss and all faculty and staff regarding their duties toward students, faculty, staff and visitors.

182. The University and the Regents failed to train and supervise their employees, agents, and/or representatives including all faculty and staff, regarding the following duties:

- a. Perceive, understand, and prevent inappropriate sexual harassment on campus;
- b. Perceive, report, and prevent inappropriate invasion of privacy campus;
- c. Provide diligent supervision to and over student athletes and other individuals, including Weiss;
- d. Thoroughly investigate any invasion of privacy by Weiss;
- e. Ensure the safety of all students, faculty, staff, and visitors to UM's campuses premises;
- f. Provide a safe environment for all students, faculty, staff, and visitors to UM's premises free from sexual harassment; and, invasions of privacy;
- g. Properly train faculty and staff to be aware of their individual responsibility for creating and maintaining a safe environment.
- h. The above list of duties is not exhaustive.

183. The University and the Regents failed to adequately train coaches, trainers, medical staff, Weiss, and others regarding the aforementioned duties which led to violations of Plaintiff's rights.

184. The University and the Regents failure to adequately train was the result of Defendants' deliberate indifference toward the well-being of student athletes.

185. The University and the Regents failure to adequately train is closely related to or actually caused Plaintiff's injuries.

186. As a result, the University and the Regents deprived Plaintiff of rights secured by the Fourteenth Amendment to the United States Constitution in violation of 42 U.S.C. § 1983.

187. Plaintiffs should be awarded all such forms of damages in this case for Regents' and the University's conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

COUNT VI – INVASION OF PRIVACY INTRUSION UPON SECLUSION

188. Plaintiffs incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

189. Plaintiffs' personal social media files, videos, and other images were each in electronic storage and were, and should have been kept, private.

190. All of that private and personal information was wrongfully accessed by Weiss.

191. Weiss's actions were not authorized.

192. The information could not have been obtained but for the Non-Individual Defendants' lack of monitoring and supervision.

193. Plaintiffs did not authorize any access.

194. Plaintiffs are embarrassed, ashamed, humiliated, and mortified that their private information has been access by total strangers and third parties.

195. Plaintiffs' social media information and image and videos are a private subject matter.

196. Plaintiffs had a right to keep all such information private.

197. The means Weiss took to obtain the information was objectively unreasonable.

198. Plaintiffs have incurred significant monetary and nonmonetary damages as a result of Defendants' actions and request the appropriate damages.

COUNT VII – GROSS NEGLIGENCE AGAINST THE REGENTS, THE UNIVERSITY, AND KEFFER

199. Plaintiffs incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

200. Plaintiffs' personal social media files, videos, and other images were each in electronic storage and were, and should have been kept, private.

201. All of that private and personal information was wrongfully accessed by Weiss.

202. Weiss's actions were not authorized.

203. The information could not have been obtained but for the Non-Individual Defendants' lack of monitoring and supervision.

204. Plaintiffs did not authorize any access.

205. Plaintiffs are embarrassed, ashamed, humiliated, and mortified that their private information has been access by total strangers and third parties.

206. Plaintiffs' social media information and image and videos are a private subject matter.

207. Plaintiffs had a right to keep all such information private.

208. Plaintiffs entrusted the Regents and the University to ensure methods were undertaken to secure, safeguard, and protect against authorized access to their private information.

209. The Regents and the University do not deny that.

210. Keffer was entrusted to keep Plaintiffs' private information private.

211. Keffer does not deny that.

212. The Non-Individual Defendants admit that Plaintiffs expected each of them to take reasonable measures to maintain the privacy of Plaintiffs' private information.

213. Each of the Non-Individual Defendants admits they are sorry for the breaches of trust that the Plaintiffs and the other victims have experienced.

214. The Regents breached their duties to Plaintiffs by failing to consider, implement, or follow a policy to oversee how or whether the University conducted its operations in a manner that would have in any manner monitored, supervised, and

ensured that retention and employment of Weiss would not result in a breach of the privacy Plaintiffs entrusted to the Regents and the University.

215. The Plaintiffs entrusted the University to take measures to secure against Weiss's unauthorized access to their private information.

216. The University failed in its executed of the duty entrusted to the University by the Plaintiffs by failing to take any action much less consider means by which to prevent the harm caused to Plaintiffs and their peers as alleged in this Complaint, including but not limited to the inaction of failing to consider, determine, enact, and implement a policy to monitor, supervise, and oversee Weiss, or ensure more than one witness or person is verifying that such sensitive and personal and private information is kept confidential.

217. The Regents were supposed to, but failed, to establish University policy, including to monitor personnel, including but not limited to Weiss, so that students on the campus are protected their privacy being invaded.

218. The University failed to provide security to Plaintiffs and to other student athletes to be able to be treated by athletic professionals who do not invade their privacy.

219. Keffer recklessly failed to ensure media and information of and pertaining to student athletes including but not limited to Plaintiffs was safely

provided and stored even after Plaintiffs and other similar to them entrusted Keffer to do so.

220. The Regents had an obligation to support Plaintiffs, and to develop the campus, its operations including student services, and admissions, and financial aid, among others, in a way that at least considered having and executing security measures to protect the personal, private, and intimate images and information of the Plaintiffs and others similar to them.

221. The Regents breached those duties because they failed to consider or implement any security measures to protect the personal, private, and intimate images and information of the Plaintiffs and others similar to them.

222. The University had a duty but failed to learn, enact, or implement any security measures to protect the personal, private, and intimate images and information of the Plaintiffs and others similar to them.

223. Keffer was reckless by failing to equip its computer systems with security that did not make it easy for Weiss to use quick, basic, and cheap internet research to invade Plaintiffs' privacy.

224. Given the sensitive nature of the Plaintiffs' private information, each of the Non-Individual Defendants knew of and, as detailed herein, breached their heightened duties to safeguard and protect Plaintiffs' privacy by failing to consider,

enact, and implement security measures, and that recklessness exposed Plaintiffs, the Class, and their intimate images.

225. The Regents' failures and omissions in these respects was so reckless that it shows a substantial lack of concern for injuries to Plaintiffs and the Class.

226. The University's failures and omissions in these respects was so reckless that it shows a substantial lack of concern for injuries to Plaintiffs and the Class.

227. Keffer's failures and omissions in these respects was so reckless that it shows a substantial lack of concern for injuries to Plaintiffs and the Class.

228. Plaintiffs have incurred significant monetary and nonmonetary damages as a result of Defendants' actions, and should be awarded damages accordingly.

COUNT VIII – NEGLIGENT HIRING

229. Plaintiffs incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

230. Plaintiffs' personal social media files, videos, and other images were each in electronic storage and were, and should have been kept, private.

231. The University had a duty to be reasonable in its review, selection, and hiring of Weiss.

232. The University was not reasonable.

233. The University failed to study, review, consider, and reasonably determine if Weiss had the kind of training, character, and respect for students to respect or at least not invade their privacy.

234. Plaintiff's private and personal information was wrongfully accessed by Weiss.

235. Weiss's actions were not authorized.

236. The information could not have been obtained but for the University's failure to consider what training to require to hire someone for the job Weiss had, but for the University's failure to consider what credentials Weiss had, but for the failure to consider Weiss's background or review it, and otherwise fail to learn and establish needed conditions that must be satisfied to hire someone to handle personal and sensitive information, or at least not to abuse the position of trust the Plaintiffs placed in the University to prudently hire someone for the job Weiss had.

237. Plaintiffs did not authorize any access by Weiss and were not asked if they thought he was fit for the job.

238. Plaintiffs are embarrassed, ashamed, humiliated, and mortified that their private information has been access by total strangers and third parties.

239. Plaintiffs' social media information and image and videos are a private subject matter.

240. Plaintiffs had a right to keep all such information private.

241. Plaintiffs entrusted the University to ensure methods were undertaken to secure, safeguard, and protect against authorized access to their private information.

242. The University does not deny that.

243. The University breached their duty to reasonably consider the credentials, training, and conditions Weiss should have had to satisfy.

244. But for that, Plaintiffs would not have been harmed.

245. But Plaintiffs were harmed.

246. The University's breach of its duty to consider much less ensure Weiss was trained to and would follow security measures to protect the personal, private, and intimate images and information of the Plaintiffs and others similar to them has caused harm to Plaintiffs.

247. Given the sensitive nature of the Plaintiffs' private information, the University knew that its hiring of Weiss should be more prudent.

248. The University failed in its duty.

249. Plaintiffs were harmed as a result.

250. Plaintiffs have incurred significant monetary and nonmonetary damages as a result of Defendants' actions and request the appropriate damages.

COUNT IX – NEGLIGENT TRAINING

251. Plaintiffs incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

252. The University had an obligation to train Weiss in a manner that would not subject the students including Plaintiffs to Weiss invading their privacy.

253. The University failed consider, study, or enact any policy, procedure, or reasonable standard that would have trained Weiss to understand the sensitivity of the information of the Plaintiffs and the Class entrusted to him and the University.

254. The University failed consider, study, or enact any policy, procedure, or reasonable standard that would have trained Weiss to understand the damage he would do if he invaded the private information of the Plaintiffs and the Class entrusted to him and the University.

255. The University of Michigan is a substantial institution and Plaintiffs reasonably expected a physician coach to be trained to care about and safeguard their personal and private information.

256. Plaintiffs understandably did not expect the University to fail to train Weiss about the highly sensitive nature of his position and leave him to his own devices to violate Plaintiffs rights and to embarrass and humiliate them.

257. The University failed to train Weiss and that failure damaged the students including but not limited to Plaintiffs.

258. The University also had an obligation, but failed, to enact and follow a policy to train Weiss to protect students such as Plaintiffs from predators.

259. But for these failures by the University, Plaintiffs would not have been damaged and would not have had her social media files, videos, and other images that were stored electronically invaded such that they no longer enjoyed privacy and freedom from viewing by others.

260. Plaintiffs have been damaged as a result.

261. Plaintiffs' social media information and image and videos are a private subject matter.

262. Plaintiffs had a right to keep all such information private.

263. The failures of the University were unreasonable.

264. Plaintiffs have incurred significant monetary and nonmonetary damages as a result of Defendants' actions and request the appropriate damages.

COUNT X – NEGLIGENT SUPERVISION

265. Plaintiffs incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

266. The University had an obligation to supervise Weiss in a manner that would not subject the students including Plaintiffs to Weiss invading their privacy.

267. The University failed consider, study, or enact any policy, procedure, or reasonable standard that would have supervised and monitored Weiss to understand

the sensitivity of the information of the Plaintiffs and the Class entrusted to him and the University.

268. The University failed consider, study, or enact any policy, procedure, or reasonable standard that would have included more secure or multiple source authorization such that Weiss would not have been able to invade Plaintiffs' privacy.

269. The University failed to consider or enact any measure to ensure a single actor such as Weiss, left unsupervised, would be able to invade the private information of the Plaintiffs and the Class.

270. The University of Michigan is a substantial institution and Plaintiffs reasonably expected a physician coach to be supervised so as to safeguard their personal and private information.

271. Plaintiffs understandably did not expect the University to fail to supervise Weiss about the highly sensitive nature of his position and leave him to his own devices to violate Plaintiffs rights and to embarrass and humiliate them.

272. The University failed to supervise Weiss, and that failure damaged the students including but not limited to Plaintiffs.

273. The University also had an obligation, but failed, to enact and follow a policy to supervise Weiss to protect students such as Plaintiffs from predators.

274. But for these failures by the University, Plaintiffs would not have been damaged and would not have had her social media files, videos, and other images

that were stored electronically invaded such that they no longer enjoyed privacy and freedom from viewing by others.

275. Plaintiffs have been damaged as a result.

276. Plaintiffs' social media information and image and videos are a private subject matter.

277. Plaintiffs had a right to keep all such information private.

278. The failures of the University were unreasonable.

279. Plaintiffs have incurred significant monetary and nonmonetary damages as a result of Defendants' actions and request the appropriate damages.

COUNT XI -- NEGLIGENT ENTRUSTMENT

280. Plaintiffs incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

281. Plaintiffs entrusted the Regents, the University, and Keffer with her private information, social media, images, and videos.

282. The Non-Individual Defendants are liable at law to Plaintiffs and the Class if they permit the handling and use of Plaintiffs' private personal information and the private and personal information of the Class to be held and handled in a manner that will cause harm to the Plaintiffs, the Class Members, or others, such as family members of the Class Member or the Plaintiffs.

283. The Non-Individual Defendants knew of the sensitivity of the information they were handling and relied heavily on their own methods and procedures for so handling the information and using the information.

284. It was a breach of a reasonable standard for the Non-Individual Defendants to not handle and use the personal and private information of the Plaintiffs with more care, attention, and sensitivity so as to safeguard and protect from instruction by Weiss.

285. The Regents, the University, and Keffer accepted Plaintiffs' entrustment, profited from the parties' relationship, and failed to safeguard Plaintiffs' private information, social media, images, and videos despite the entrustment to them.

286. The Regents, the University, and Keffer had a heightened duty to keep Plaintiffs' personal social media files, videos, and other images were electronic communications private.

287. The Regents failed in that duty.

288. The University failed in that duty.

289. Keffer failed in that duty.

290. Plaintiffs' information was accessed by Weiss.

291. The Non-Individual Defendants failed to seriously or reasonably consider how to safeguard Plaintiffs' information and the information of other Class Members.

292. The Non-Individual Defendants failed to carry out their heightened duty to take actions to safeguard and ensure the privacy of Plaintiffs' personal and private information.

293. The Non-Individual Defendants each breached their duties by failing to undertake any expected maintenance, protection, monitoring, and supervision to confirm Plaintiffs' personal and private information was safe.

294. But for the Non-Individual Defendants' negligent entrustment, Plaintiffs would not have been damaged.

295. Plaintiffs' social media information and image and videos are a private subject matter.

296. Plaintiffs had a right to keep all such information private.

297. Plaintiffs have incurred significant monetary and nonmonetary damages as a result of Defendants' actions and request the appropriate damages.

COUNT XII – NEGLIGENT RETENTION

298. Plaintiffs incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

299. Plaintiffs' personal social media files, videos, and other images were private.

300. The University has had a history of athletic department invasions and assaults on the privacy of student athletes.

301. The University had a duty to retain Weiss only if he would not continue that unfortunate history.

302. The University had an obligation to retain Keffer only if it would safeguard Plaintiffs' private information.

303. The University was warned historically about threats from outside vendors to invade the privacy of student athletes.

304. The University was warned historically about the threats from personnel of the leaders of the athletic department that trainers can be threats to the invasion of the privacy of student athletes.

305. Despite those warnings, and the experiences of the University and the Regents historically, the Regents and the University hired and retained Weiss and he violated the Plaintiffs' privacy and the privacy of others.

306. Despite those warnings, and the experiences of the University and the Regents historically, the Regents and the University hired and retained Keffer and it failed to take any reasonable action to safeguard the Plaintiffs' privacy and the privacy of others.

307. The University failed take any action to ensure that Weiss was working in an ethical manner that did not invade the privacy of Plaintiffs.

308. The University failed to take any action to ensure that Keffer stored Plaintiffs's personal and private information in a manner that would not be accessed by others.

309. But for the failures to retain Weiss and Keffer in a prudent and safe manner, Plaintiffs would not have been harmed.

310. Plaintiffs had a right to keep all her information private.

311. The lack of review or any legitimate historical basis to retain Keffer and Weiss was objectively unreasonable.

312. Plaintiffs have incurred significant monetary and nonmonetary damages as a result of Defendants' actions and request the appropriate damages.

COUNT XIII – TRESPASS TO CHATTELS

313. Plaintiffs incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

314. By accessing Plaintiffs' personal and private information without authorization, Weiss and the University intentionally and harmfully interfered with, and wrongfully exercised dominion or control over, Plaintiffs' private and personal information, images, videos, and social media.

315. The aforementioned accessing, dominion, and control was willful and malicious.

316. Plaintiffs and the Class have incurred significant monetary and nonmonetary damages as a result of Weiss's and the University's intentional and harmful interference with, and wrongful exercise of dominion or control over, Plaintiffs' private and personal information.

317. Plaintiffs are entitled to exemplary damages as a result of these intentional and harmful act and interference with, and wrongful exercise of control over, their property.

COUNT XIV – COMMON LAW CONVERSION

318. Plaintiffs incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

319. By accessing Plaintiffs's personal and private information, Weiss and the University wrongfully exercised dominion or control over Plaintiffs's property, social media, images, videos, and related media, and that access was in denial of, or inconsistent with, Plaintiffs' rights therein.

320. The aforementioned exercise of dominion or control was willful and malicious.

321. Plaintiffs have incurred significant monetary and nonmonetary damages as a result of these Defendants wrongfully exercising dominion or control

over Plaintiffs' personal and private information all of which was in denial of, or inconsistent with, Plaintiffs' rights therein.

322. Plaintiffs are entitled to exemplary damages as a result of these Weiss and the University wrongfully exercising dominion or control over Plaintiffs' property, in denial of, or inconsistent with, Plaintiffs' rights therein.

COUNT XV – VIOLATIONS OF MCL § 600.2919a

323. Plaintiffs incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

324. MCL § 600.2919a provides:

(1) A person damaged as a result of either or both of the following may recover 3 times the amount of actual damages sustained, plus costs and reasonable attorney fees:

(a) Another person's stealing or embezzling property or converting property to the other person's own use.

(b) Another person's buying, receiving, possessing, concealing, or aiding in the concealment of stolen, embezzled, or converted property when the person buying, receiving, possessing, concealing, or aiding in the concealment of stolen, embezzled, or converted property knew that the property was stolen, embezzled, or converted.

(2) The remedy provided by this section is in addition to any other right or remedy the person may have at law or otherwise.

325. Plaintiffs were damaged as a result of the University and Weiss possessing, concealing, aiding the concealment of, stealing, and/or embezzling Plaintiffs' private and personal information and converting that information, those videos, and those images to those Defendants' own use by using that information for their own purposes.

326. Under MCL § 600.2919a, Plaintiffs are entitled to 3 times actual damages, plus costs and reasonable attorney fees.

WHEREFORE, Plaintiffs request that the Court enter a judgment encompassing the relief requested above, plus significant compensatory damages exceeding \$100,000,000.00 together with costs, interest and attorney fees, against Defendants, and such other relief to which they are entitled

Date: March 21, 2025

Respectfully Submitted,

By: s/Parker Stinar

Parker Stinar

Mike Grieco (Pro Hac Vice Forthcoming)

**STINAR GOULD GRIECO &
HENSLEY, PLLC**

101 N. Wacker Dr., Floor M,
Suite 100

Chicago, Illinois 60606

T: (312) 728-7444

parker@sgghlaw.com

Counsel for Plaintiffs

CLOSED, reassigned

**U.S. District Court
Eastern District of Michigan (Detroit)
CIVIL DOCKET FOR CASE #: 2:25-cv-10855-MAG-EAS**

****CASE CLOSED ALL ENTRIES MUST BE MADE IN 25-cv-10806.**** Doe I et al v. Weiss et al

Assigned to: District Judge Mark A. Goldsmith

Referred to: Magistrate Judge Elizabeth A. Stafford

Cause: 28:1331 Fed. Question

Date Filed: 03/26/2025

Date Terminated: 05/23/2025

Jury Demand: Plaintiff

Nature of Suit: 440 Civil Rights: Other

Jurisdiction: Federal Question

Plaintiff

Jane Doe

I - 53

represented by **Brendan John Childress**

Hurwitz Law PLLC

617 Detroit St.

Suite 125

Ann Arbor, MI 48104

248-933-5121

Email: brendan@hurwitzlaw.com

ATTORNEY TO BE NOTICED

Jonathan R. Marko

Marko Law, PLLC

220 W. Congress

4th Floor

Detroit, MI 48226

313-777-7529

Fax: 313-470-2011

Email: jon@markolaw.com

ATTORNEY TO BE NOTICED

Yana A. Hart

Clarkson Law Firm

22525 Pacific Coast Highway

Malibu, CA 90265

213-788-4050

Email: yhart@clarksonlawfirm.com

ATTORNEY TO BE NOTICED

Noah S. Hurwitz

Hurwitz Law PLLC

1514 Creal Cres

Ann Arbor, MI 48103

734-645-5263

Email: noah@hurwitzlaw.com

ATTORNEY TO BE NOTICED

Plaintiff

McKenzie Johnson

represented by **Brendan John Childress**

(See above for address)

ATTORNEY TO BE NOTICED

Noah S. Hurwitz

(See above for address)

ATTORNEY TO BE NOTICED

Plaintiff

Sarah Caldarola

represented by **Noah S. Hurwitz**

(See above for address)

ATTORNEY TO BE NOTICED

Plaintiff

Jenna Schilling

represented by **Noah S. Hurwitz**

(See above for address)

ATTORNEY TO BE NOTICED

V.

Defendant

Matthew Weiss

Defendant

University of Michigan Board of Regents

represented by **Daniel B. Tukel**

Butzel Long

201 West Big Beaver Road

Suite 1200

Troy, MI 48084

313-225-7047

Email: tukel@butzel.com

ATTORNEY TO BE NOTICED

Sheldon H. Klein

Butzel

201 West Big Beaver Road

Suite 1200

Troy, MI 48084

248-258-1414

Fax: 248-258-1439

Email: klein@butzel.com

ATTORNEY TO BE NOTICED

Defendant

University of Michigan

represented by **Daniel B. Tukel**

(See above for address)

ATTORNEY TO BE NOTICED

Sheldon H. Klein

(See above for address)

ATTORNEY TO BE NOTICED

Defendant

Keffer Development Services, LLC

represented by **Carl Andrew Fejko**

Dillon McCandless King Coulter Graham

Civil Practice

128 West Cunningham St.
Butler, PA 16001
724-822-2148
Email: cfejko@dmkcg.com
ATTORNEY TO BE NOTICED

Jordan P. Shuber

Dillon McCandless King Coulter &
Graham, LLP
128 West Cunningham Street
Butler, PA 16001
724-283-2200
Fax: 724-283-2298
Email: jshuber@dmkcg.com
ATTORNEY TO BE NOTICED

Thomas W. King , III

Dillon McCandless King Coulter & Graham
LLP
128 West Cunningham Street
Buter, PA 16001
724-283-2200
Email: tking@dmkcg.com
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
03/26/2025	<u>1</u>	COMPLAINT filed by All Plaintiffs against All Defendants with Jury Demand. Plaintiff requests summons issued. Receipt No: AMIEDC-10173316 - Fee: \$ 405. County of 1st Plaintiff: Out of State - County Where Action Arose: Washtenaw - County of 1st Defendant: Washtenaw. [Previously dismissed case: No] [Possible companion case(s): None] (Hurwitz, Noah) (Entered: 03/26/2025)
03/27/2025		A United States Magistrate Judge of this Court is available to conduct all proceedings in this civil action in accordance with 28 U.S.C. 636c and FRCP 73. The Notice, Consent, and Reference of a Civil Action to a Magistrate Judge form is available for download at http://www.mied.uscourts.gov (JBro) (Entered: 03/27/2025)
03/27/2025	<u>2</u>	SUMMONS Issued for *Matthew Weiss* (JBro) Modified on 3/27/2025 (JBro). [DOCKETING ERROR. SUMMONS NOT ATTACHED] (Entered: 03/27/2025)
03/27/2025	<u>3</u>	SUMMONS Issued for *Matthew Weiss* (JBro) (Entered: 03/27/2025)
03/27/2025	<u>4</u>	SUMMONS Issued for *The Regents Of The University Of Michigan* (JBro) (Entered: 03/27/2025)
03/27/2025	<u>5</u>	SUMMONS Issued for *The University of Michigan* (JBro) (Entered: 03/27/2025)
03/27/2025	<u>6</u>	SUMMONS Issued for *Keffer Development Services, LLC* (JBro) (Entered: 03/27/2025)
03/27/2025	<u>7</u>	NOTICE of Appearance by Jonathan R. Marko on behalf of All Plaintiffs. (Marko, Jonathan) (Entered: 03/27/2025)
03/28/2025	<u>8</u>	NOTICE of Appearance by Daniel B. Tukel on behalf of The Regents Of The University Of Michigan, The University of Michigan. (Tukel, Daniel) (Entered: 03/28/2025)

03/31/2025	<u>9</u>	ORDER REASSIGNING CASE from District Judge Linda V. Parker and Magistrate Judge Kimberly G. Altman to District Judge Mark A. Goldsmith and Magistrate Judge David R. Grand. (SSch) (Entered: 03/31/2025)
04/01/2025	<u>10</u>	STIPULATED ORDER EXTENDING TIME TO RESPOND TO COMPLAINT (Response due by 6/2/2025) - Signed by District Judge Mark A. Goldsmith. (CCie) (Entered: 04/01/2025)
04/02/2025	<u>11</u>	NOTICE of Appearance by Brendan John Childress on behalf of All Plaintiffs. (Childress, Brendan) (Entered: 04/02/2025)
04/09/2025	<u>12</u>	ORDER OF RECUSAL AND REASSIGNING CASE from Magistrate Judge David R. Grand to Magistrate Judge Anthony P. Patti. (NAhm) (Entered: 04/09/2025)
04/10/2025	<u>13</u>	CORRECTED ORDER OF RECUSAL AND REASSIGNING CASE from Magistrate Judge David R. Grand to Magistrate Judge Elizabeth A. Stafford. (NAhm) (Entered: 04/10/2025)
04/13/2025	<u>14</u>	AMENDED COMPLAINT with Jury Demand filed by All Plaintiffs against All Defendants. NEW PARTIES ADDED. (Hurwitz, Noah) (Entered: 04/13/2025)
04/13/2025	<u>15</u>	MOTION for Preliminary Injunction by All Plaintiffs. (Attachments: # <u>1</u> Exhibit Ex. 1, CBS News Detroit University of Michigan Says Hackers Gained Personal Information of Individuals in Cyberattack, # <u>2</u> Exhibit Ex. 2, Emails from University of Michigan Police and the University of Michigan Privacy Office) (Childress, Brendan) (Entered: 04/13/2025)
04/15/2025	<u>16</u>	NOTICE of Appearance by Sheldon H. Klein on behalf of University of Michigan, University of Michigan Board of Regents. (Klein, Sheldon) (Entered: 04/15/2025)
04/15/2025	<u>17</u>	NOTICE by Jane Doe from 10806 (Attachments: # <u>1</u> Exhibit) (Stinar, Parker) (Entered: 04/15/2025)
04/16/2025	<u>18</u>	NOTICE by University of Michigan, University of Michigan Board of Regents <i>of filing Motion to Consolidate in case 25-cv-10806</i> (Tukel, Daniel) (Entered: 04/16/2025)
04/16/2025	<u>19</u>	CERTIFICATE of Service/Summons Returned Executed. Keffer Development Services, LLC served on 4/7/2025, answer due 4/28/2025. (Hurwitz, Noah) (Entered: 04/16/2025)
04/22/2025	<u>20</u>	ORDER Regarding Status Conference. Signed by District Judge Mark A. Goldsmith. (HRya) (Entered: 04/22/2025)
04/22/2025	<u>21</u>	NOTICE TO APPEAR REMOTELY: Status Conference set for 5/14/2025 at 9:00 AM before District Judge Mark A. Goldsmith. (HRya) (Entered: 04/22/2025)
04/22/2025	<u>22</u>	STIPULATED ORDER Staying Time for Response to <u>15</u> MOTION for Preliminary Injunction. Signed by District Judge Mark A. Goldsmith. (HRya) (Entered: 04/22/2025)
04/23/2025	<u>23</u>	NOTICE by All Plaintiffs <i>of Filing Motion for Staus Conference</i> (Thompson, Jason) (Entered: 04/23/2025)
04/23/2025	<u>24</u>	AMENDED COMPLAINT with Jury Demand filed by All Plaintiffs against All Defendants. NEW PARTIES ADDED. (Hurwitz, Noah) (Entered: 04/23/2025)
04/24/2025	<u>25</u>	WAIVER OF SERVICE Returned Executed. Keffer Development Services, LLC waiver sent on 4/24/2025, answer due 6/23/2025. (Hurwitz, Noah) (Entered: 04/24/2025)
04/24/2025	<u>26</u>	NOTICE by Jane Doe from 10806 <i>Majority Plaintiffs' Amended Motion</i> (Stinar, Parker) (Entered: 04/24/2025)

05/06/2025	27	NOTICE by All Plaintiffs re 23 Notice (Other) <i>Corrected Notice of Filing Motion for Status Conference</i> (Thompson, Jason) (Entered: 05/06/2025)
05/14/2025	28	NOTICE of Appearance by Thomas W. King, III on behalf of Keffer Development Services, LLC. (King, Thomas) (Entered: 05/14/2025)
05/14/2025		Minute Entry for remote proceedings before District Judge Mark A. Goldsmith: Status Conference held on 5/14/2025. (Court Reporter: None Present, Not on the Record) (JHea) (Entered: 05/14/2025)
05/14/2025	29	NOTICE of Appearance by Carl Andrew Fejko on behalf of Keffer Development Services, LLC. (Fejko, Carl) (Entered: 05/14/2025)
05/15/2025	30	NOTICE of Appearance by Jordan P. Shuber on behalf of Keffer Development Services, LLC. (Shuber, Jordan) (Entered: 05/15/2025)
05/16/2025	31	NOTICE by Jane Doe re: <i>Supplemental Memorandum in Support of Plaintiff Counsels Motion for Appointment of Interim Class Counsel</i> (Attachments: # 1 Exhibit A) (Hart, Yana) (Entered: 05/16/2025)
05/23/2025	32	ORDER FOR CONSOLIDATION AND RELATED MATTERS. Signed by District Judge Mark A. Goldsmith. (JHea) (Entered: 05/23/2025)
05/23/2025	33	Notice to Parties Regarding Consolidated Case: Order of consolidation entered on *5/23/2025*. Designated lead case number is *25-10806*. (JHea) (Entered: 05/23/2025)

PACER Service Center			
Transaction Receipt			
06/05/2025 16:26:06			
PACER Login:	ThomaKingtking	Client Code:	
Description:	Docket Report	Search Criteria:	2:25-cv-10855-MAG-EAS
Billable Pages:	4	Cost:	0.40

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION**

JANE DOE 1 and JANE DOE 2, on behalf
of themselves and others similarly situated,

Plaintiffs,

Case No.

v.

Hon.

MATTHEW WEISS; the REGENTS
OF THE UNIVERSITY OF MICHIGAN;
the UNIVERSITY OF MICHIGAN;
KEFFER DEVELOPMENT SERVICES,
LLC,

Defendants.

Jonathan R. Marko (P72450)
MARKO LAW, PLLC
Attorneys for Plaintiff
220 W. Congress, 4th Floor
Detroit, MI 48226
(313) 777-7529
jon@markolaw.com

Noah S. Hurwitz (P74063)
HURWITZ LAW PLLC
Attorneys for Plaintiff
340 Beakes St., Suite 125
Ann Arbor, MI 48104
(844) 487-9489
noah@hurwitzlaw.com

There is no other pending or resolved civil action arising out
of the transaction or occurrence alleged in this Complaint.

PLAINTIFFS' CLASS ACTION COMPLAINT

Pursuant to Fed. R. Civ. P. 15(a)(2), Plaintiffs JANE DOE 1 and JANE DOE 2 (“Plaintiffs”), through their attorneys, **MARKO LAW, PLLC** and **HURWITZ LAW PLLC**, for their Complaint against MATTHEW WEISS, the REGENTS OF THE UNIVERSITY OF MICHIGAN, the UNIVERSITY OF MICHIGAN, and KEFFER DEVELOPMENT SERVICES, LLC, state as follows:

INTRODUCTION

Student-athletes at the University of Michigan entrusted private and sensitive information to the University with the expectation that they would be protected and safeguarded from the potentially dangerous actions of athletic department employees who interact daily with student-athletes and have influence upon them. Only a massive failure of oversight would allow for one of the University’s highest paid employees, an Offensive Coordinator of the Michigan football team, to use his position of highest authority to terrorize the heart of the University Michigan Athletic Department, its student-athletes. After years of investigation and countless inquiries, the University of Michigan still refuses to acknowledge and communicate with victims of these heinous crimes. Matthew Weiss’ extensive cyber assault on Plaintiffs’ basic privacy rights is horrible, but it is the University of Michigan and its privacy vendors who have failed to protect vulnerable student-athletes whose most private information now resides in the public domain.

JURISDICTION AND VENUE

1. Plaintiff Jane Doe 1 was a student-athlete at the University of Michigan from 2020 to 2024, was a member of the Michigan Women’s Volleyball team., and resides in Union County, New Jersey.

2. Plaintiff Jane Doe 2 was a student-athlete at the University of Michigan from 2020 to 2024, was a member of the Michigan Women’s Soccer team, and resides in Washtenaw County, Michigan.

3. The Regents of the University of Michigan (the “Regents”) is a corporate entity with the authority to be sued and is responsible for governing the University, as per Mich. Comp. Laws § 390.3 and § 390.4.

4. The University of Michigan (the “University”) is a public institution established under the laws of the State of Michigan.

5. The University has received and continues to receive state funding, making it subject to Michigan state laws.

6. Keffer Development Services, LLC (“Keffer”) is a Pennsylvania-based limited liability company that has consistently conducted business in Michigan by directly providing services to residents and entities within the state, thereby availing itself of Michigan's legal protections.

7. The wrongful conduct and legal violations committed by Keffer, as outlined in this complaint, specifically affected Plaintiffs who resided in Michigan at the time of the incidents.

8. Matthew Weiss (“Weiss”) is an individual residing in Michigan.

9. This Court has jurisdiction under 28 U.S.C. §§ 1331 and 1367, as this case involves a claim under the Stored Communications Act, 18 U.S.C. § 2701(a) *et seq.*, supplemental jurisdiction over additional related claims under 28 U.S.C. § 1367(a), and subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d) because this is a class action in which the amount in controversy exceeds \$5,000,000, there are more than 100 putative class members, and the majority of putative class members are citizens of a state different than the state of which Defendants are citizens.

10. Venue is proper in this district under 28 U.S.C. § 1391, as a substantial portion of the events giving rise to these claims occurred within this jurisdiction, and the Defendants are subject to personal jurisdiction here.

11. Plaintiffs’ injuries are redressable by monetary compensation and all of Plaintiffs’ alleged injuries and those of the class members, are fairly traceable to Defendants’ conduct

12. Plaintiffs are timely filing a Notice of Intent to File Claims in the Court of Claims (“COC”) pursuant to MCL 600.6431.

INDIVIDUAL ALLEGATIONS

13. Plaintiffs Jane Doe 1 and 2 were female student-athletes at the University of Michigan at all relevant times in which Weiss was employed by the University.

14. Upon information and belief, Plaintiffs Jane Doe 1 and 2 fell victim to Defendants' conduct when Weiss unlawfully captured their private and sensitive personal records from electronic mail sources without permission.

15. Weiss primarily targeted female college athletes, so he posed a greater threat to Plaintiffs Jane Doe 1 and 2 who were prominent female student-athletes at the University of Michigan.

16. Weiss targeted Jane Doe 1 and 2 by infiltrating athlete databases that were maintained by Defendant Keffer, from which he gained access to by virtue of his elevated level of access as an Offensive Coordinator for the Michigan football team.

INDIVIDUAL AND CLASS ALLEGATIONS

17. Weiss was employed by the University.

18. Weiss' conduct occurred during his employment at the University.

19. The Regents had a responsibility to oversee the University's operations and ensure it upheld ethical standards and protected its students.

20. This duty of care was violated when the Regents and University personnel failed to adequately supervise Weiss, resulting in the unlawful invasion of privacy affecting Plaintiffs and thousands of others.

21. Plaintiffs are current and former student-athletes at the University and other affected institutions who were specifically targeted and harmed due to this violation of their privacy by Defendants.

22. The Regents were also charged with managing the University's policies, financial operations, and strategic decisions, including budget approvals, tuition determination, and infrastructure development.

23. They failed in this obligation by neglecting to implement or enforce policies that would have ensured proper oversight of University personnel, including Weiss, thereby preventing the breach of privacy that affected Plaintiffs.

24. The Regents did not take any measures to prevent the harm inflicted upon Plaintiffs and other students as outlined in this Complaint.

25. The Regents had the responsibility to establish University policies ensuring the monitoring of personnel in positions of authority, such as Weiss who was the Offensive Coordinator of the Michigan football team, but failed to do so, thereby exposing students to privacy violations.

26. The Regents and the University were required to ensure that student-athletes had access to services from professionals who would respect their privacy.

27. The Regents and the University acted recklessly by not ensuring that student-athletes' personal and sensitive information, including that of Plaintiffs, was securely managed, despite being entrusted to do so.

28. The Regents and the University have a duty to support Plaintiffs and take appropriate security measures to protect private information and images.

29. They breached this duty by failing to consider or implement any meaningful security measures to safeguard Plaintiffs' sensitive personal data.

30. As financial stewards of the University, the Regents and the University failed to responsibly allocate resources by prioritizing cost avoidance over implementing security measures that could have prevented the privacy breaches.

31. The Regents, responsible for overseeing all University of Michigan campuses, failed to enforce policies that could have detected, investigated, or prevented Weiss' unlawful actions, which were facilitated by the University's access provisions.

32. The University, like the Regents, failed to uphold these responsibilities and engaged in similar breaches of duty.

33. Plaintiffs entrusted the University to protect their private images and information.

34. The University neglected this heightened responsibility, recklessly allowing Weiss to access and exploit the private information and images of Plaintiffs and other student-athletes.

35. The Regents also had general oversight authority over the University's expenditures, yet failed to ensure that public funds were allocated to establish security protocols that would have protected student-athletes' private information.

36. The University employed Weiss and had authority over him.

37. The University assigned and directed Weiss' job responsibilities.

38. These job duties enabled Weiss to access and exploit private, intimate information and images of Plaintiffs and others, which had been entrusted to the University for safekeeping.

39. Despite providing Weiss with the means to invade Plaintiffs' privacy, the University failed to supervise or monitor his actions.

40. The University betrayed the trust of Plaintiffs and others by granting Weiss electronic credentials that allowed him to surveil student-athletes, including Plaintiffs, and access their personal information and images.

41. Without any University oversight, Weiss, in the course of his employment, unlawfully accessed and exploited Plaintiffs' private data.

42. The Regents, the University, and Weiss engaged in misconduct, recklessness, and wrongdoing, which also implicated Keffer.

43. Keffer's negligence and reckless disregard contributed to Weiss' privacy violations against Plaintiffs and their fellow student-athletes.

44. Keffer had agreed to securely store and manage Plaintiffs' sensitive data, ensuring it remained inaccessible to University employees like Weiss and unauthorized third parties.

45. Keffer was aware that the information it stored for Plaintiffs and others was private, personal, and sensitive.

46. Keffer had an explicit obligation to protect this sensitive data but failed to fulfill this duty.

47. By failing to implement any policies, procedures, or security measures, Keffer breached its duty to protect the private information entrusted to it by Plaintiffs and others.

48. As a direct result of Keffer's security failures, Weiss was able to access Plaintiffs' private, personal, and intimate images and information.

49. Keffer collects personal data about students and student-athletes.

50. The University and the Regents sanctioned Keffer's collection of this private information.

51. Plaintiffs trusted that the University and the Regents' authorization of Keffer's role would ensure the safety and confidentiality of their data.

52. The Regents and the University took no action to ensure that Keffer maintained the privacy of Plaintiffs' sensitive information.

53. The Regents' negligence in this regard directly harmed Plaintiffs.

54. The University's failure to safeguard this data also caused harm to Plaintiffs.

55. Keffer failed to implement measures to protect Plaintiffs' private information, leading to its unauthorized access.

56. Keffer took no precautions to prevent Weiss from accessing Plaintiffs' personal information and images.

57. Due to the negligence and recklessness of Keffer, the Regents, and the University, Weiss was able to unlawfully obtain and misuse sensitive information belonging to Plaintiffs and others.

58. Between approximately 2015 and January 2023, Weiss unlawfully accessed the digital accounts of over 3,300 individuals, including Plaintiffs and other University student-athletes, as detailed in the criminal indictment against him.

59. Weiss was able to do so because the University and the Regents granted him access credentials, enabling him to obtain and misuse private images and information.

60. The Non-Individual Defendants failed to monitor Weiss' activities, supervise his conduct, review his employment status, or ensure that his job duties were performed in a manner that respected Plaintiffs' privacy.

61. The Non-Individual Defendants failed to implement even basic security measures such as multi-factor authentication, background checks, peer oversight, or routine audits to protect student-athletes' private information.

62. As a result of these failures, Weiss was able to unlawfully access private, intimate information belonging to Plaintiffs and their peers, which was maintained by Keffer and authorized for collection by the University and the Regents.

63. The careless, negligent, and improper actions of the Regents, the University, and Keffer facilitated Weiss' ability to target female college athletes and access their private and sensitive information without authorization, including but not limited to the Plaintiffs.

64. The Non-Individual Defendants were aware that Weiss, due to his job responsibilities, had a significant advantage in accessing private information and the personal privacy interests of the Plaintiffs and their peers.

65. The Regents, the University, and Keffer failed to implement reasonable security measures or conduct background checks on Weiss, which allowed him to freely research, target, and invade the privacy of multiple University athletes,

67. Due to the recklessness of the University, the Regents, and the gross negligence of Keffer, Weiss was able to download personal and intimate digital photographs and videos of Plaintiffs and other class members who had entrusted this information to the Non-Individual Defendants.

69. Because the Non-Individual Defendants failed to monitor Weiss, he was able to compile detailed records on individuals whose private photographs and videos he sought to obtain. Their failure to implement protective measures was so

severe that Weiss even documented comments regarding the bodies and sexual preferences of Plaintiffs and their peers.

70. The information that Weiss acquired due to the Non-Individual Defendants' negligence is highly confidential, personal, and distressing when exposed without authorization, causing humiliation and embarrassment.

71. Weiss accessed, without authorization or exceeding authorization, student-athlete databases from over 100 colleges and universities nationwide, maintained by Keffer.

72. Thousands of students remain at risk because, despite decades of complaints and reports of misconduct within athletic departments, the University, the Regents, and Keffer repeatedly failed to review how Plaintiffs' personal data was stored, maintained, and accessed.

73. The University and the Regents neglected to investigate Keffer's protocols or implement safeguards regarding Keffer's work with students and their private images, failing to uphold their duty to protect entrusted personal data.

74. The University and the Regents also failed to explore or establish preventive measures to shield students from Weiss' actions.

75. Neither the University nor the Regents have provided any explanation or justification for their failure to review Keffer's contract, investigate Keffer's

practices, implement oversight mechanisms, or consider measures to prevent students' exposure to Weiss.

76. Due to the lack of control and enabling behavior of the Non-Individual Defendants, Weiss was able to gain unauthorized access to databases containing highly sensitive and private information belonging to Plaintiffs and others.

77. Many, if not all, of these databases were maintained by Keffer and were entrusted to him with the expectation of being securely safeguarded.

78. Plaintiffs entrusted the University and the Regents to ensure that Keffer adequately protected their private information and images.

79. Defendants completely failed to implement or execute any reasonable security measures that could have safeguarded Plaintiffs' private information from Weiss' unauthorized access.

80. Exploiting unsecured databases, Weiss downloaded personally identifiable information (PII) and medical records of more than 150,000 athletes, including Plaintiffs.

81. Weiss also downloaded athlete passwords used to access Keffer's computer system to view and update their data, including Plaintiffs' credentials.

82. The athletes' passwords were encrypted but were poorly secured due to the Non-Individual Defendants' recklessness. Consequently, Weiss, who was left unsupervised, managed to crack the encryption using basic internet research.

83. Through open-source research, Weiss further investigated targeted athletes, such as Plaintiffs, collecting personal details like their mothers' maiden names, pets' names, birthplaces, and nicknames—information Plaintiffs had entrusted to the Non-Individual Defendants but which was inadequately protected.

84. Using a combination of data obtained from student-athlete databases and additional research, Weiss, due to the lack of oversight by the Non-Individual Defendants, was able to gain access to over 2,000 athletes' social media, email, and cloud storage accounts, including those belonging to Plaintiffs.

85. Once inside these accounts, Weiss searched for and downloaded private and intimate photographs and videos that were not publicly available.

86. Weiss also accessed, without authorization, the social media, email, and cloud storage accounts of more than 1,300 additional students and alumni from universities across the country, including Plaintiffs, due to the reckless disregard for their safety and privacy by the Non-Individual Defendants.

87. Upon accessing these accounts, Weiss extracted personal and intimate content.

88. The Regents, University, and Keffer have also failed to take any steps to address or remedy the harm and privacy violations they allowed to occur.

89. Weiss exploited weaknesses in account authentication processes to gain further access to additional accounts of students and alumni, leveraging this access to infiltrate more social media, email, and cloud storage accounts.

90. The Regents, University, and Keffer failed to take preventive action against such unauthorized access.

91. The Non-Individual Defendants were long aware that the type of data Weiss accessed was expected to remain private and that any breach would cause significant harm. Despite this knowledge, they failed to implement appropriate safeguards to protect the confidential information entrusted to them by Plaintiffs and other student-athletes.

92. From approximately 2015 to January 2023, Weiss intentionally accessed, without authorization, personal and private information belonging to Plaintiffs and others, including data stored on university servers, social media, email, and cloud platforms.

93. Weiss unlawfully obtained digital photographs, videos, and personal data from more than 3,300 individuals, including Plaintiffs, violating privacy laws in Michigan, Maryland, and Pennsylvania.

94. Weiss took advantage of security vulnerabilities and the lack of supervision by the Non-Individual Defendants to reset account passwords, access private accounts, and further compromise Plaintiffs' digital security.

95. As a direct result of the negligence, recklessness, and misconduct of the Non-Individual Defendants, Plaintiffs have suffered substantial financial and emotional damages exceeding \$75,000, exclusive of costs, interest, and legal fees.

96. Plaintiffs file this lawsuit both individually and as a class action on behalf of all those similarly affected under Rule 23.

97. This case meets the requirements of numerosity, commonality, predominance, typicality, and adequacy as outlined in the rule.

98. The Class is currently defined as: All individuals whose personal data, images, social media, or videos were accessed by Weiss without authorization (referred to as “Class Members”).

99. Numerosity: While the exact number of Class Members is not currently known and will be determined through further discovery, it is significant enough to make individual joinder impractical.

100. Law enforcement officials have confirmed that there are a substantial number of victims, satisfying the numerosity requirement.

101. Resolving the claims of these Class Members in a single action will benefit all parties and the Court by conserving resources, preventing inconsistent rulings, and providing a fair and efficient method for adjudication.

102. Class Members can be readily identified through information and records held by federal and state authorities, the Regents, the University, and Keffer.

103. Electronic records maintained by the Non-Individual Defendants, who conducted their own investigations, can confirm the identities of Class Members.

104. Commonality: The evidence establishing how, when, where, and through what means Plaintiffs and other Class Members experienced these invasions is best evaluated collectively.

105. Defendants' actions, inactions, negligence, and recklessness apply uniformly to all Plaintiffs and Class Members.

106. Weiss' unauthorized downloads and access to private information through insecure systems affected all Class Members in essentially the same manner, causing identical types of harm.

107. The majority of legal and factual issues relevant to Plaintiffs and Class Members are common and take precedence over any individual matters.

108. Plaintiffs' claims are representative of those of the Class Members, as they share a common origin in terms of timing, circumstances, and harm suffered.

109. Plaintiffs are well-suited to represent the class, as they are committed to seeking justice and adequately reflect the harm experienced by the Class Members.

110. Pursuing this case as a class action is the most effective approach, facilitating the fair administration of justice because:

- a. Separate lawsuits by individual Class Members could lead to inconsistent rulings, imposing conflicting obligations on Defendants.
- b. Many victims may not come forward unless a class is certified.
- c. Comprehensive equitable relief—including monitoring, protection, therapy, and other necessary measures—can be appropriately provided for the entire Class.
- d. A class action is the most practical and manageable way to address these claims.
- e. Without a class action, individual Class Members may remain unaware of whether they were recorded, where their private images are stored, or who may have access to them, leaving their injuries unresolved.
- f. Individual Class Members may have little incentive or ability to pursue separate legal actions on their own.

**COUNT I – VIOLATION OF THE COMPUTER FRAUD
AND ABUSE ACT – 18 U.S.C. § 1030**

111. Plaintiffs restate and incorporate the allegations outlined above as if fully set forth herein.

112. Weiss violated the Computer Fraud and Abuse Act by unlawfully accessing Plaintiffs’ private information without authorization.

113. He did so in the course of his assigned job responsibilities at the University.

114. Weiss’ actions constitute a violation of the Act because he “knowingly accessed a computer without authorization” and/or “exceeded authorized access, thereby obtaining... information.” 18 U.S.C. § 1030(a)(2)(C).

115. Under the law, Weiss qualifies as an “inside hacker” since he initially accessed a computer system with legitimate credentials as part of his work with Plaintiffs and Class Members in their capacity as student-athletes. However, he then surpassed the scope of his permitted access by entering restricted areas of the digital network.

116. This situation is comparable to opening your office door only to discover an unauthorized individual inside. If the intruder is an unknown person with no right to be in the building, they are completely unauthorized. If it’s a colleague from a different department, they have exceeded their permitted access.

117. Weiss’ actions were deliberate, as he was fully aware that he was not authorized to access the restricted information but did so regardless, with the University’s implicit approval.

118. The University is vicariously liable for Weiss’ actions, as he conducted them while performing his duties as a medical sports staff member within the University’s athletic department.

119. Legal precedent establishes that an employer is responsible for the wrongful acts committed by its agents in the course of their employment.

120. Under 18 U.S.C. § 1030(g), Plaintiffs are entitled to seek damages from Weiss and the University through this civil action, as well as injunctive or other equitable relief.

121. Given the willful violations committed by Weiss and the University, which resulted in significant harm, humiliation, and distress to Plaintiffs and the Class, Plaintiffs should be awarded all appropriate damages in this case.

COUNT II – VIOLATIONS OF THE STORED COMMUNICATIONS ACT

122. Plaintiffs restate and incorporate the allegations outlined above as if fully set forth herein.

123. The Stored Communications Act, 18 U.S.C. § 2701 et seq., prohibits the unauthorized access of web-based cloud storage, media accounts, and other digital platforms, including those maintained by Keffer, which contained highly personal, private, and sensitive information belonging to Plaintiffs and others in similar situations.

124. Specifically, under 18 U.S.C. § 2701(a), it is unlawful for any person to (1) knowingly and intentionally access, without authorization, a system through which an electronic communication service is provided; or (2) intentionally exceed authorized access to such a system and, in doing so, obtain, modify, or obstruct authorized access to electronic communications while they are stored in that system.

125. Plaintiffs' digital communications and personal information were electronically stored and clearly fall within the scope of the statute's protections.

126. Weiss accessed Plaintiffs' private data—including messages, files, and media—without authorization while performing duties associated with his role at the University.

127. His actions in accessing Plaintiffs' data without permission were deliberate and undertaken knowingly in connection with his employment.

128. Plaintiffs' private messages, files, and media could not have been accessed without unauthorized entry, and such access would not have occurred had Weiss not been employed by the University in his specific role within sports medicine.

129. Under Section 2707 of the Stored Communications Act, individuals affected by violations of this statute are entitled to pursue civil action.

130. This law imposes strict liability on violators.

131. The statute permits affected individuals to seek remedies including equitable and declaratory relief, actual damages (or statutory damages of at least \$1,000 per violation), punitive damages, as well as reasonable attorneys' fees and litigation expenses, pursuant to 18 U.S.C. § 2707(b)-(c).

132. Weiss and the University's unauthorized access to Plaintiffs' private information, including messages, files, and media, constituted a violation of 18 U.S.C. § 2701(a).

133. Both Weiss and the University were fully aware that they had no legal authority to access this data but did so regardless.

134. Their intentional misconduct led to multiple violations of the Stored Communications Act.

135. As a result of these violations, Plaintiffs have suffered significant financial and non-financial harm and seek appropriate compensation for their damages.

136. Under the statute, Plaintiffs are entitled to recover either (1) their actual damages combined with any profits gained by Weiss and the University from the violations or (2) statutory damages of at least \$1,000 per violation.

137. Given the deliberate nature of these violations, the Court should impose punitive damages against the Defendants.

138. Plaintiffs are also entitled to reimbursement for reasonable attorneys' fees and legal costs.

COUNT III – VIOLATION OF TITLE IX, 20 U.S.C. § 1681(A) et seq.

139. Plaintiffs restate and incorporate the allegations outlined above as if fully set forth herein.

140. Title IX mandates that “No person in the United States shall, on the basis of sex, be ... subjected to discrimination under any education program or activity receiving Federal financial assistance ...”

141. Each Plaintiff qualifies as a "person" under the statutory language of Title IX.

142. Weiss specifically targeted women in his unwarranted privacy violations, constituting sex-based discrimination.

143. The University receives federal financial support for its educational programs, making it subject to Title IX of the Education Amendments of 1972, 20 U.S.C. § 1681(a), et seq.

144. Under Title IX, the University is obligated to investigate allegations of sexual harassment.

145. The University was aware of the highly sensitive nature of the Plaintiffs' private and personal information, which Weiss was able to access due to his position.

146. The University and Regents displayed deliberate indifference to sexual harassment by:

- a. Failing to protect Plaintiffs and others in accordance with Title IX requirements;
- b. Neglecting to properly investigate and address concerns regarding the deeply private information Plaintiffs entrusted to them;
- c. Not implementing corrective measures to prevent Weiss from engaging in further sexual harassment of students; and
- d. Failing to investigate additional acts of deliberate indifference adequately.

147. The University and Regents' failure to respond appropriately to sexual harassment was clearly unreasonable given the known circumstances, constituting deliberate indifference.

148. Due to the University's inadequate protection, investigation, and response to the harassment of female students, Plaintiffs have been effectively denied equal educational opportunities, including access to medical care and athletic training.

149. At the time Plaintiffs received certain medical training services from the University, they were unaware that the Defendants had failed to properly consider their safety in relation to Weiss' hiring, training, and supervision.

150. As a direct result of the deliberate indifference shown by the University and Regents, Plaintiffs have suffered a loss of educational benefits and opportunities.

151. Plaintiffs have incurred and will continue to incur attorneys' fees and litigation costs.

152. At the time of Defendants' wrongful conduct, Plaintiffs were either unaware or, despite reasonable diligence, could not have been aware of the institutional failures of Defendants concerning their Title IX obligations.

153. The University and Regents maintained a policy and/or practice of deliberate indifference toward the protection of female student-athletes.

154. This policy and/or practice of disregarding female athletes' privacy rights contributed to an increased risk of sexual harassment.

155. Despite having the power to prevent these privacy violations and acts of harassment, Defendants failed to do so.

156. Due to the University's and Regents' policy and/or practice of deliberate indifference, Plaintiffs were subjected to privacy invasions and sexual harassment by Weiss.

157. Plaintiffs should be awarded damages for the substantial harm, humiliation, and distress caused by the University's and Regents' actions and inactions.

**COUNT IV -- VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C. § 1983 –
STATE CREATED DANGER**

158. Plaintiffs restate and incorporate the allegations outlined above as if fully set forth herein.

159. The Fourteenth Amendment's Due Process Clause prohibits the state from depriving individuals of life, liberty, or property without due process of law.

160. The Regents and the University knowingly and recklessly exposed Plaintiffs to a dangerous individual, Weiss, despite being aware of his potential to inflict serious harm through sexual harassment and violations of their privacy.

161. Plaintiffs, as female student-athletes, were foreseeable victims of such misconduct.

162. The violation of Plaintiffs' privacy rights was entirely foreseeable.

163. The Regents and the University took affirmative actions that deprived Plaintiffs of a safe campus environment, thereby creating or heightening the risk of harm and leading to both physical and emotional suffering.

164. The University and the Regents demonstrated a reckless disregard for Plaintiffs' safety.

165. Through their decisions and actions, the University and the Regents failed to provide a secure campus, directly contributing to Plaintiffs' exposure to harm and emotional distress.

166. The University and the Regents willfully neglected their duty to safeguard Plaintiffs.

167. Plaintiffs are entitled to recover all applicable damages for the Regents' and the University's actions, which caused severe harm, humiliation, and emotional distress to Plaintiffs and the Class.

COUNT V – FAILURE TO TRAIN AND SUPERVISE 42 U.S.C. § 1983

168. Plaintiffs restate and incorporate the allegations outlined above as if fully set forth herein.

169. The University and the Regents bore the ultimate responsibility and authority to train and oversee their employees, agents, and representatives, including

Weiss, as well as all faculty and staff, in fulfilling their duties toward students, faculty, staff, and visitors.

170. The University and the Regents neglected to properly train and supervise their employees, agents, and representatives, including all faculty and staff, regarding their obligations, which included but were not limited to:

- a. Recognizing, addressing, and preventing incidents of sexual harassment on campus;
- b. Identifying, reporting, and preventing unauthorized invasions of privacy on campus;
- c. Ensuring diligent oversight of student athletes and other individuals, including Weiss;
- d. Conducting thorough investigations into any privacy invasions committed by Weiss;
- e. Safeguarding all students, faculty, staff, and visitors on UM's campus premises;
- f. Maintaining a campus environment free from sexual harassment and invasions of privacy;
- g. Providing adequate training to faculty and staff regarding their individual responsibility in fostering and upholding a safe campus environment.

171. The University and the Regents failed to sufficiently educate and train coaches, trainers, medical staff, Weiss, and other relevant personnel regarding the aforementioned responsibilities, which ultimately resulted in violations of Plaintiffs' rights.

172. The failure of the University and the Regents to provide adequate training stemmed from their deliberate indifference toward the safety and well-being of student athletes.

173. This lack of proper training directly contributed to or was the cause of Plaintiffs' injuries.

174. Consequently, the University and the Regents deprived Plaintiffs of rights protected under the Fourteenth Amendment to the United States Constitution, constituting a violation of 42 U.S.C. § 1983.

175. Plaintiffs are entitled to full compensation for the harm, distress, and humiliation they endured due to the Regents' and the University's actions and inaction.

COUNT VI – INVASION OF PRIVACY INTRUSION UPON SECLUSION
(As to Defendant Weiss)

176. Plaintiffs restate and incorporate the allegations outlined above as if fully set forth herein.

177. Plaintiffs' personal social media content, videos, and other images were stored electronically and were intended to remain private.

178. Weiss unlawfully accessed this private and personal information.

179. His actions were unauthorized.

180. This information would not have been obtained had the Non-Individual Defendants properly monitored and supervised access.

181. Plaintiffs never granted permission for such access.

182. Plaintiffs feel embarrassed, ashamed, humiliated, and deeply distressed that their private information has been exposed to strangers and third parties.

183. Plaintiffs' social media data, images, and videos are inherently private.

184. Plaintiffs had a rightful expectation that this information would remain confidential.

185. The methods Weiss used to access the information were objectively unreasonable.

186. As a result of Defendant's actions, Plaintiffs have suffered substantial financial and emotional harm and seek appropriate compensation.

COUNT VII – GROSS NEGLIGENCE
(As to Defendant Weiss)

187. Plaintiffs restate and incorporate the allegations outlined above as if fully set forth herein.

188. Plaintiffs' personal social media content, including files, videos, and images, were stored electronically and were meant to remain private.

189. Weiss unlawfully accessed Plaintiffs' private and personal information.

190. Weiss acted without authorization.

191. Plaintiffs never granted permission for such access.

192. Plaintiffs feel deep embarrassment, shame, humiliation, and distress knowing that their private information has been exposed to strangers and third parties.

193. Plaintiffs' social media content, including images and videos, is inherently private.

194. Plaintiffs had a fundamental right to maintain the confidentiality of this information.

195. As a direct result of Defendants' actions, Plaintiffs have suffered both financial and non-financial harm and are entitled to appropriate compensation.

COUNT VIII – NEGLIGENT HIRING OF KEFFER

196. Plaintiffs restate and incorporate the allegations outlined above as if fully set forth herein.

197. Plaintiffs' personal social media files, videos, and other images were stored electronically and should have remained private.

198. The University neglected to evaluate, review, and assess whether Weiss possessed the necessary training, character, and respect for students to ensure their privacy was upheld and not violated.

199. Weiss wrongfully accessed Plaintiffs' private and personal information.

200. Weiss' actions were unauthorized.

201. This unauthorized access occurred due to the University's failure to establish appropriate hiring and training standards for Weiss' role, failure to verify his credentials, failure to conduct a thorough background review, and failure to implement safeguards to ensure that individuals handling sensitive information were properly vetted and did not abuse their position of trust.

202. Plaintiffs never consented to Weiss' access and were never consulted regarding his fitness for the position.

203. Plaintiffs feel embarrassed, ashamed, humiliated, and distressed knowing that their private information has been accessed by strangers and third parties.

204. Plaintiffs' social media content, images, and videos are highly personal and private.

205. Plaintiffs had a fundamental right to keep such information confidential.

206. Plaintiffs relied on the University to take appropriate measures to secure, safeguard, and prevent unauthorized access to their private information.

207. The University acknowledges this responsibility.

208. The University failed in its duty to adequately assess Weiss' credentials, training, and the necessary qualifications for his role.

209. Had the University fulfilled this duty, Plaintiffs would not have suffered harm.

210. However, Plaintiffs did suffer harm.

211. The University's negligence in failing to ensure Weiss was properly trained and would adhere to security measures protecting Plaintiffs' sensitive and private information directly resulted in harm.

212. Given the highly sensitive nature of Plaintiffs' personal data, the University was aware that it needed to exercise greater diligence in its hiring process.

213. The University failed in this responsibility.

214. As a result, Plaintiffs suffered harm.

215. Plaintiffs have endured significant financial and emotional damages due to Defendants' actions and seek appropriate compensation.

COUNT IX – NEGLIGENT TRAINING, SUPERVISION, AND
ENTRUSTMENT, AND RETENTION
(As to Defendant University of Michigan)

216. Plaintiffs restate and incorporate the allegations outlined above as if fully set forth herein.

217. The University neglected to evaluate, establish, or enforce any policies, procedures, or reasonable safeguards that would have educated Weiss on the harm caused by invading Plaintiffs' and the Class's private information.

218. As a prominent institution, the University of Michigan led Plaintiffs to reasonably expect that a coach would be properly trained to respect and protect their personal and private information.

219. Plaintiffs reasonably did not anticipate that the University would fail to provide Weiss with proper training on the sensitive nature of his role, leaving him unchecked and enabling him to violate Plaintiffs' rights, causing them humiliation and distress.

220. The University's failure to train Weiss resulted in harm to students, including Plaintiffs.

221. Additionally, the University had a duty—but failed—to develop and enforce a policy to ensure Weiss was trained to protect students like Plaintiffs from predatory behavior.

222. The University's failures were unreasonable.

223. The University had a duty to oversee Weiss in a way that would prevent him from violating students' privacy, including that of Plaintiffs.

224. The University neglected to assess, implement, or establish any policy, procedure, or reasonable safeguard that would have ensured proper oversight and monitoring of Weiss in handling the sensitive information entrusted to him by Plaintiffs and the Class.

225. As a well-established institution, the University of Michigan led Plaintiffs to reasonably expect that a coach would be adequately supervised to protect their personal and private information.

226. Plaintiffs had no reason to anticipate that the University would fail to properly oversee Weiss, leaving him unchecked in a position of trust where he could violate Plaintiffs' rights, causing them embarrassment and humiliation.

227. The University was also obligated—but failed—to implement and follow a policy ensuring Weiss was properly supervised to protect students like Plaintiffs from potential predators.

228. Had the University fulfilled its responsibilities, Plaintiffs would not have suffered harm, nor would their electronically stored social media files, videos, and images have been accessed without their consent, violating their privacy.

229. The University has a history of privacy invasions and misconduct within its athletic department, including incidents affecting student-athletes.

230. The University had a responsibility to retain Weiss only if he would not perpetuate that troubling history.

231. The University was obligated to retain Keffer only if it ensured the protection of Plaintiffs' private information.

232. The University had previously been warned about the risks posed by external vendors who could compromise student-athletes' privacy.

233. The University had also been cautioned about the potential threats posed by its own athletic department personnel, including trainers, in violating student-athletes' privacy.

234. Despite these warnings and the University's prior experiences, the Regents and the University proceeded to hire and retain Weiss, who ultimately violated Plaintiffs' privacy along with that of others.

235. Plaintiffs have suffered significant financial and non-financial harm due to Defendants' actions and seek appropriate compensation.

COUNT X – TRESPASS TO CHATTELS
(As to Defendant Weiss)

236. Plaintiffs restate and incorporate the allegations outlined above as if fully set forth herein.

237. Weiss and the University intentionally and unlawfully accessed Plaintiffs' private and personal information, including images, videos, and social media, thereby wrongfully asserting control over and interfering with their sensitive data without authorization.

238. This unauthorized access and control were deliberate and carried out with malicious intent.

239. As a direct result of Weiss' and the University's intentional misconduct, Plaintiffs and the Class have suffered substantial financial and non-financial harm.

240. Plaintiffs are entitled to exemplary damages due to the intentional, harmful interference with, and wrongful exertion of control over, their private and personal information.

COUNT XI – VIOLATIONS OF MCL § 600.2919a
(As to Defendants Weiss & Keffer)

241. Plaintiffs restate and incorporate the allegations outlined above as if fully set forth herein.

242. Michigan Compiled Laws (MCL) § 600.2919a states:

(1) An individual who suffers harm due to either or both of the following may recover three times the amount of actual damages sustained, along with costs and reasonable attorney fees:

(a) Another individual stealing, embezzling, or wrongfully converting property for their own use.

(b) Another individual purchasing, receiving, possessing, concealing, or assisting in the concealment of stolen, embezzled, or converted property, with knowledge that the property was unlawfully obtained.

(2) The remedy provided under this statute is supplemental to any other legal or equitable right or remedy available.

243. Plaintiffs suffered harm due to the University and Weiss acquiring, concealing, assisting in the concealment of, stealing, and/or misappropriating Plaintiffs' private and personal information. They also wrongfully used Plaintiffs' images, videos, and data for their own benefit.

244. Pursuant to MCL § 600.2919a, Plaintiffs are entitled to recover three times the actual damages sustained, in addition to costs and reasonable attorney fees.

COUNT XII – ASSAULT
(As to Defendant Weiss)

245. Plaintiffs restate and incorporate the allegations outlined above as if fully set forth herein.

246. Defendant’s conduct, in accessing Plaintiffs’ personal and private information as outlined above, was intentional.

247. Defendant’s conduct was without consent or legal justification.

248. Defendant’s conduct caused a reasonable apprehension of imminent harm to Plaintiffs.

249. As a result of Defendant’s conduct, Plaintiffs suffered severe damages.

**COUNT XIII – INTENTIONAL INFLICTION
OF EMOTIONAL DISTRESS**
(As to Defendant Weiss)

250. Plaintiffs restate and incorporate the allegations outlined above as if fully set forth herein.

251. Defendant’s conduct, in accessing Plaintiffs’ personal and private information as outlined above, was intentional.

252. Defendant’s conduct was extreme and outrageous.

253. Defendant’s conduct was not for any proper purpose.

254. Defendant’s conduct caused severe emotional distress to Plaintiffs.

255. Plaintiffs suffered severe emotional distress and economic damage as a result of Defendant's intentional actions.

**COUNT XIV – VIOLATION OF THE MICHIGAN IDENTITY THEFT
PROTECTION ACT – MCL 445.61 et. seq.**

256. Plaintiffs restate and incorporate the allegations outlined above as if fully set forth herein.

257. Plaintiffs' personal social media content, videos, and other images were stored electronically and were intended to remain private.

258. Weiss unlawfully accessed this private and personal information.

259. His actions were unauthorized.

260. Defendants maintained a database of Plaintiffs' sensitive information.

261. Defendants had a duty to notify Plaintiffs of the unauthorized breach of their deeply private data.

262. Defendants, however, failed to do so.

263. As a result, Plaintiffs were completely unaware for years that their highly sensitive, private data was being accessed without their authorization in violation of Michigan's Identity Theft Protection Act.

264. As a result of Defendants' conduct, Plaintiffs have suffered severe damages.

WHEREFORE, Plaintiffs respectfully request the Honorable Court to enter judgment against Defendants in an amount that will fully and fairly compensate them

for their damages; for costs of this action; for pre- and post-judgment interest; attorney fees; and for all other just and proper relief.

Respectfully submitted,

/s/ Jonathan R. Marko

Jonathan R. Marko (P72450)

MARKO LAW, PLLC

Attorneys for Plaintiff

220 W. Congress, 4th Floor

Detroit, Michigan 48226

P: (313) 777-7529 / F: (313) 771-5785

jon@markolaw.com

/s/ Noah S. Hurwitz

Noah S. Hurwitz (P74063)

Hurwitz Law, PLLC

Attorneys for Plaintiff

340 Beakes Street, Suite 125

Ann Arbor, MI 48103

Dated: March 26, 2025

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION**

JANE DOE 1 and JANE DOE 2, on behalf
of themselves and others similarly situated,

Plaintiffs,

Case No.

v.

Hon.

MATTHEW WEISS; the REGENTS
OF THE UNIVERSITY OF MICHIGAN;
the UNIVERSITY OF MICHIGAN;
KEFFER DEVELOPMENT SERVICES,
LLC,

Defendants.

Jonathan R. Marko (P72450)
MARKO LAW, PLLC
Attorneys for Plaintiff
220 W. Congress, 4th Floor
Detroit, MI 48226
(313) 777-7529
jon@markolaw.com

Noah S. Hurwitz (P74063)
HURWITZ LAW PLLC
Attorneys for Plaintiff
340 Beakes St., Suite 125
Ann Arbor, MI 48104
(844) 487-9489
noah@hurwitzlaw.com

JURY DEMAND

Plaintiffs, by and through their attorneys, hereby demand a trial by jury of the
issues in the above-captioned case.

Respectfully submitted,

/s/ Jonathan R. Marko

Jonathan R. Marko (P72450)

MARKO LAW, PLLC

Attorneys for Plaintiff

220 W. Congress, 4th Floor

Detroit, Michigan 48226

P: (313) 777-7529 / F: (313) 771-5785

jon@markolaw.com

/s/ Noah S. Hurwitz

Noah S. Hurwitz (P74063)

Hurwitz Law, PLLC

Attorneys for Plaintiff

340 Beakes Street, Suite 125

Ann Arbor, MI 48103

Dated: March 26, 2025

**U.S. District Court
Eastern District of Michigan (Detroit)
CIVIL DOCKET FOR CASE #: 2:25-cv-10988-MAG-EAS**

****CASE CLOSED ALL ENTRIES MUST BE MADE IN 25-cv-10806.**** Doe v. Weiss et al

Assigned to: District Judge Mark A. Goldsmith
Referred to: Magistrate Judge Elizabeth A. Stafford
Demand: \$75,000
Cause: 28:1331 Fed. Question

Date Filed: 04/07/2025
Date Terminated: 05/23/2025
Jury Demand: Plaintiff
Nature of Suit: 440 Civil Rights: Other
Jurisdiction: Federal Question

Plaintiff

Jane Doe

represented by **Yana A. Hart**
Clarkson Law Firm
22525 Pacific Coast Highway
Malibu, CA 90265
213-788-4050
Email: yhart@clarksonlawfirm.com
ATTORNEY TO BE NOTICED

Robert J. Lantzy
Buckfire & Buckfire
29000 Inkster Road
Ste. 150
Southfield, MI 48034
248-569-4646
Email: robert@buckfirelaw.com
ATTORNEY TO BE NOTICED

Plaintiff

Jane Doe 2

represented by **Robert J. Lantzy**
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Jane Doe 3

represented by **Robert J. Lantzy**
(See above for address)
ATTORNEY TO BE NOTICED

V.

Defendant

Matthew Weiss

Defendant

Regents of the University of Michigan

represented by **Daniel B. Tukel**
Butzel Long
201 West Big Beaver Road
Suite 1200

Troy, MI 48084
313-225-7047
Email: tukel@butzel.com
ATTORNEY TO BE NOTICED

Sheldon H. Klein
Butzel
201 West Big Beaver Road
Suite 1200
Troy, MI 48084
248-258-1414
Fax: 248-258-1439
Email: klein@butzel.com
ATTORNEY TO BE NOTICED

Defendant

University of Michigan

represented by **Daniel B. Tukel**
(See above for address)
ATTORNEY TO BE NOTICED

Sheldon H. Klein
(See above for address)
ATTORNEY TO BE NOTICED

Defendant

Keefer Development Services, LLC

represented by **Carl Andrew Fejko**
Dillon McCandless King Coulter Graham
Civil Practice
128 West Cunningham St.
Butler, PA 16001
724-822-2148
Email: cfejko@dmkcg.com
ATTORNEY TO BE NOTICED

Jordan P. Shuber
Dillon McCandless King Coulter &
Graham, LLP
128 West Cunningham Street
Butler, PA 16001
724-283-2200
Fax: 724-283-2298
Email: jshuber@dmkcg.com
ATTORNEY TO BE NOTICED

Thomas W. King , III
Dillon McCandless King Coulter & Graham
LLP
128 West Cunningham Street
Buter, PA 16001
724-283-2200
Email: tking@dmkcg.com
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
04/07/2025	1	COMPLAINT <i>and Jury Demand</i> filed by Jane Doe 1 against Jane Doe 1 with Jury Demand. Plaintiff requests summons issued. Receipt No: AMIEDC-10187529 - Fee: \$ 405. County of 1st Plaintiff: Aransas - County Where Action Arose: Washtenaw - County of 1st Defendant: Washtenaw. [Previously dismissed case: No] [Possible companion case(s): None] (Lantzy, Robert) Modified on 4/8/2025 (LHam). [COMPLAINT IS DOE VS. WEISS ET AL] (Entered: 04/07/2025)
04/08/2025	2	SUMMONS Issued for * All Defendants * (LHam) (Entered: 04/08/2025)
04/09/2025	3	NOTICE of Appearance by Daniel B. Tukel on behalf of Regents of the University of Michigan, University of Michigan. (Tukel, Daniel) (Entered: 04/09/2025)
04/10/2025	4	STIPULATED ORDER Extending Time to Respond to Complaint 1 , (Response due by 6/2/2025). Signed by District Judge Denise Page Hood. (LSau) (Entered: 04/10/2025)
04/10/2025	5	AMENDED COMPLAINT with Jury Demand filed by All Plaintiffs against All Defendants. NO NEW PARTIES ADDED. (Lantzy, Robert) (Entered: 04/10/2025)
04/14/2025	6	ORDER REASSIGNING CASE from District Judge Denise Page Hood and Magistrate Judge Curtis Ivy, Jr to District Judge Mark A. Goldsmith and Magistrate Judge Elizabeth A. Stafford. (SSch) (Entered: 04/14/2025)
04/15/2025	7	NOTICE of Appearance by Sheldon H. Klein on behalf of Regents of the University of Michigan, University of Michigan. (Klein, Sheldon) (Entered: 04/15/2025)
04/15/2025	8	NOTICE by Jane Doe from 10806 (Attachments: # 1 Exhibit) (Stinar, Parker) Modified on 4/16/2025 (LHam). [NOTICE OF MOTION TO CONSOLIDATE WITH CASE 25-10806 AND NOTICE TO APPOINT LEAD COUNSEL] (Entered: 04/15/2025)
04/16/2025	9	NOTICE by Regents of the University of Michigan, University of Michigan <i>of filing Motion to Consolidate in case 25-cv-10806</i> (Tukel, Daniel) (Entered: 04/16/2025)
04/22/2025	10	ORDER Regarding Status Conference. Signed by District Judge Mark A. Goldsmith. (HRya) (Entered: 04/22/2025)
04/22/2025	11	NOTICE TO APPEAR REMOTELY: Status Conference set for 5/14/2025 at 9:00 AM before District Judge Mark A. Goldsmith. (HRya) (Entered: 04/22/2025)
04/23/2025	12	NOTICE by All Plaintiffs <i>of Filing Motion for Staus Conference</i> (Thompson, Jason) (Entered: 04/23/2025)
04/24/2025	13	NOTICE by Jane Doe from 10806 <i>Majority Plaintiffs' Amended Motion</i> (Stinar, Parker) (Entered: 04/24/2025)
04/25/2025	14	WAIVER OF SERVICE Returned Executed. Jane Doe 2 waiver sent on 4/25/2025, answer due 6/24/2025; Jane Doe 3 waiver sent on 4/25/2025, answer due 6/24/2025; Jane Doe waiver sent on 4/25/2025, answer due 6/24/2025. (Lantzy, Robert) Modified on 4/25/2025 (LHam).[AS TO KEEFER DEVELOPMENT SERVICES, LLC] (Entered: 04/25/2025)
05/06/2025	15	NOTICE by All Plaintiffs re 12 Notice (Other) <i>Corrected Notice of Filing Motion for Status Conference</i> (Thompson, Jason) (Entered: 05/06/2025)
05/12/2025	16	NOTICE of Joinder/Concurrence in by Jane Doe 2, Jane Doe 3, Jane Doe (Lantzy, Robert) (Entered: 05/12/2025)
05/14/2025	17	NOTICE of Appearance by Thomas W. King, III on behalf of Keefer Development Services, LLC. (King, Thomas) (Entered: 05/14/2025)

05/14/2025	18	NOTICE of Appearance by Carl Andrew Fejko on behalf of Keefer Development Services, LLC. (Fejko, Carl) (Entered: 05/14/2025)
05/14/2025		Minute Entry for remote proceedings before District Judge Mark A. Goldsmith: Status Conference held on 5/14/2025. (Court Reporter: None Present, Not on the Record) (JHea) (Entered: 05/14/2025)
05/15/2025	19	NOTICE of Appearance by Jordan P. Shuber on behalf of Keefer Development Services, LLC. (Shuber, Jordan) (Entered: 05/15/2025)
05/16/2025	20	NOTICE by Jane Doe re: <i>Supplemental Memorandum in Support of Plaintiff Counsels Motion for Appointment of Interim Class Counsel</i> (Attachments: # 1 Exhibit A) (Hart, Yana) (Entered: 05/16/2025)
05/23/2025	21	ORDER FOR CONSOLIDATION AND RELATED MATTERS. Signed by District Judge Mark A. Goldsmith. (JHea) (Entered: 05/23/2025)
05/23/2025	22	Notice to Parties Regarding Consolidated Case: Order of consolidation entered on *5/23/2025*. Designated lead case number is *25-10806*. (JHea) (Entered: 05/23/2025)

PACER Service Center			
Transaction Receipt			
06/05/2025 16:29:36			
PACER Login:	ThomaKingtking	Client Code:	
Description:	Docket Report	Search Criteria:	2:25-cv-10988-MAG-EAS
Billable Pages:	4	Cost:	0.40

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

JANE DOE 1,

Plaintiff,

vs.

MATTHEW WEISS; the REGENTS
OF THE UNIVERSITY OF
MICHIGAN; the UNIVERSITY OF
MICHIGAN; KEFFER
DEVELOPMENT SERVICES, LLC,

Defendants.

Case No. ____

Hon. _____

Mag.

Jury Trial Demanded

PLAINTIFF'S COMPLAINT AND JURY DEMAND

Plaintiff, JANE DOE 1 (“Plaintiff” or “Plaintiff(s)), through her attorneys, Buckfire Law Firm, for her Complaint against MATTHEW WEISS, the REGENTS OF THE UNIVERSITY OF MICHIGAN, the UNIVERSITY OF MICHIGAN, and KEFFER DEVELOPMENT SERVICES, LLC, states as follows:

THE PARTIES, JURISDICTION, AND VENUE

1. Plaintiff Jane Doe 1 was a student athlete at the University of Michigan between 2012 and 2016 and was a member of a University of Michigan Women’s sports team.
2. Plaintiff Jane Doe 1 is domiciled in the State of Texas.
3. The Regents of the University of Michigan (the “Regents”) is a corporate entity,

with the right to be sued, and is responsible for governing the University of Michigan, pursuant to Mich. Comp. Laws § 390.3 and § 390.4.
4. The University of Michigan (the “University”) is a public university organized and existing under the laws of the State of Michigan.
5. The University has received and continues to receive state financial assistance and is therefore, among other reasons, subject to the laws of the State of Michigan.
6. Keffer Development Services, LLC (“Keffer”) is a Pennsylvania limited liability company that has continuously and systematically done business in the State of Michigan through its direct providing of services to residents and entities

within the State of Michigan, thereby purposefully availing itself of protections of the laws of the State of Michigan.

7. Keffer's misconduct and legal failures as detailed in this Complaint occurred specifically with respect to the Plaintiff(s) who reside in Michigan, resided in Michigan or were otherwise subject to Keffer's misconduct during the time of the incidents alleged in this Complaint.

8. Matthew Weiss is an individual who resides in Michigan or resided in Michigan at the time of the alleged misconduct.

JURISDICTION

9. Jurisdiction is proper in this Court under 28 U.S.C. §§ 1331 and 1367 because this matter involves a cause of action under the Stored Communications Act, 18 U.S.C. § 2701(a) *et seq.*; the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; Title IX, 20 U.S.C. § 1681(A) *et seq.*; 42 U.S.C. § 1983; the Fourth Amendment of the U.S. Constitution; and the Fourteenth Amendment of the U.S. Constitution, and the court has supplemental jurisdiction of the other causes of action under 28 U.S.C. § 1367(a).

10. Venue is appropriate in this district under 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in this district and Defendants are subject to personal jurisdiction in this district.

11. Plaintiff(s)' injuries are redressable by monetary compensation.

COMMON ALLEGATIONS

12. Weiss was employed by the University of Michigan between approximately

2021 and 2023.

13. Weiss's actions were in furtherance of his job duties for the University.

14. The Regents had a responsibility and duty to ensure that the University operates with integrity and care for the students and others.

15. Keffer had a responsibility and duty to protect the private data of student athletes and others stored within their database and to have mechanisms in place to prevent such an invasion of privacy and other conduct occurred in this case.

16. The Regents breached that duty by failing to supervise and monitor Weiss and as a result Plaintiff(s) and thousands of others have had their privacy illegally invaded.

17. The Regents are also responsible for overseeing the University's operations, finances, and policy, including approving budgets, tuition rates, IT policies, and construction projects.

18. The Regents also failed in that duty by failing to consider, implement, or follow a policy to oversee how or whether the University conducted its operations in a manner that would have in any manner monitored, supervised, and ensured that retention and employment of Weiss would not result in a breach of the privacy Plaintiff(s) and others entrusted to the University.

19. The Regents also failed in that duty by failing to take any action much less consider means by which to prevent the harm caused to Plaintiff(s) and others as alleged in this Complaint.

20. The Regents were supposed to, but failed, to establish University policies, including monitoring of personnel, such as Weiss, so that students and others on the campus or off campus were protected from their privacy being invaded through electronic or other means.

21. The Regents were required but failed to ensure that the University offered services such as to have student athletes and others be able to be treated by athletic professionals and others do not invade their privacy and to ensure that students and others electronic media was secure from invasion by unauthorized third-parties.

22. The Regents recklessly failed to ensure media and information of and pertaining to student athletes and others including but not limited to Plaintiff(s) was safely secured because Plaintiff(s) and others similar to them entrusted the Regents to do so.

23. The Regents had an obligation to support Plaintiff(s), and to develop the campus, its operations including student services, IT policies and procedures, among others, in a way that considered having and executing security measures to protect the personal, private, and intimate images and information of the Plaintiff(s) and others similar to them.

24. The Regents breached those duties because they failed to consider or implement any security measures to protect the personal, private, and intimate images and information of the Plaintiff(s) and others similar to them.

25. The Regents were responsible for financial oversight of the University but failed to prudently exercise that duty because they placed avoiding cost of learning, having, and implementing security measures to protect the personal, private, and intimate images and information of the Plaintiff(s) and others similar to them, as more important than incurring the cost of establishing and paying for programs to so implement safety policies, and to monitor and ensure student safety including information electronically stored.

26. The Regents are supposed to regulate all three U-M campuses but failed to do so by failing to consider or implement any policies to review, discover, or prevent the willful invasions of privacy committed by Weiss as a result of the access the University provided to him to so invade the privacy of the student athletes including but not limited to Plaintiff(s) who entrusted themselves to the University and the Regents.

27. The University itself had all of the same duties as the Regents.

28. The University itself breached all of the same duties and in the same and/or similar manners as the Regents.

29. The Plaintiff(s) and others like them entrusted the University to safeguard their bodily images and other electronically stored or accessible information.

30. The University breached the heightened duty it had and recklessly permitted Weiss to invade the Plaintiff(s)' privacy and likewise for their student

athlete peers and expose them and their intimate images.

31. The Regents also had and breached general supervision privileges and obligations to “control” and “direct” all expenditures of funds but failed to ensure any of the funds given or available to the University were used to study, select, and implement safety measures to protect student athletes’, and others private and personal body images and information, particularly female athletes, while at the same time spending money on other expenses that are wholly unrelated to student athlete, and others health, safety, and privacy.

32. The University employed Weiss.

33. The University controlled Weiss.

34. The University assigned and directed job duties to and upon Weiss.

35. Those job duties and direction directly resulted in Weiss accessing private, personal, intimate images and information of Plaintiff(s) and others similar to them, all of which were private, and entrusted to be safeguarded by the university and its agents.

36. The University took no action to monitor Weiss despite providing him with the ability and means to invade Plaintiff(s)’ privacy and the privacy of others.

37. The University breached the confidences that Plaintiff(s) and others similar to Plaintiff(s) entrusted to the University and did so by providing Weiss with the electronic credentials and ability to track and spy on students athletes including Plaintiff(s), and to use those credentials to invade Plaintiff(s)’ private lives and

obtain and use images of them and personal information relating to them.

38. With no University supervision, and during execution of his official duties as an employee of the University, Weiss invaded Plaintiff(s)' privacy and the privacy of others in similar postures through means provided to Weiss by the University.

39. The misconduct, recklessness, and bad acts of the Regents, the University, and Weiss also included and involved Keffer.

40. Keffer's misconduct, negligence, and recklessness also contributed to Weiss invading the privacy of Plaintiff(s) and their fellow student athletes and others.

41. Keffer had an express obligation to safeguard and protect the personal, private, and intimate images and information entrusted to Keffer by Plaintiff(s) and others similar to them.

42. Keffer agreed to safely maintain and store information, images, expressions, and videos of Plaintiff(s) and their peers in secure manner, free from access from employees of the University such as Weiss or other unauthorized third parties.

43. Keffer knew that the images and information of Plaintiff(s) and others similar to them would include personal, private, and intimate information.

44. Keffer knowingly and intentionally took on the obligation to safeguard and protect the personal, private, and intimate images and information entrusted to

Keffer by Plaintiff(s) and others similar to them.

45. Keffer breached those obligations by failing to consider, enact, or implement any policy, procedure, or security measure to safeguard and protect the personal, private, and intimate images and information entrusted to Keffer by Plaintiff(s) and others similar to them.

46. As a direct result of Keffer's security failures, negligence and gross negligence, Weiss accessed the personal, private, and intimate images and information entrusted to Keffer by Plaintiff(s) and others similar to them.

47. Keffer collects information including private information about students and student athletes.

48. The University and the Regents authorized Keffer's collection of that information that is and was personal and private in nature.

49. Plaintiff(s) and others similar to them entrusted that the Regents and the University's authorization to and entrustment to Keffer would keep them safe and their private images and information private.

50. The Regents and the University failed to take any action to ensure that Keffer retained the privacy of the images and information of Plaintiff(s) and others like them.

51. The Regents' failures in this respect harmed Plaintiff(s).

52. The University's failures in this respect harmed Plaintiff(s).

53. Keffer failed to take any action necessary to ensure that it retained the

privacy of the images and information of Plaintiff(s) and others like them entrusted to Keffer.

54. Keffer failed to consider or take any action necessary to protect against the access by Weiss of the private information, images, expressions, and videos of Plaintiff(s) and their peers.

55. Due to the negligent and reckless conduct of Keffer, the Regents, and the University (collectively, the “Non-Individual Defendants”), Weiss was able to, among other misconduct, invade the privacy of various individuals including but not limited to Plaintiff(s) and their peers.

56. Between approximately 2015 and January 2023, as was detailed in the federal criminal indictment against him, Weiss gained access—without and in excess of authorization—to the social media, email, and/or cloud storage accounts of more than 3,300 people including but not limited to University student athletes and others, past and present, and including but not limited to Plaintiff(s).

57. His ability to do so was aided by the University and the Regents both of whom permitted him to have access and use of electronic credentials that were means of viewing and downloading personal, private, and intimate images of Plaintiff(s) and others similar to them.

58. The Non-Individual Defendants failed to review Weiss’s activity, failed to supervise his activity, failed to review his retention in a prudent manner, and failed to ensure his work duties were being undertaken and completed with respect for

Plaintiff(s)' privacy and the privacy of others.

59. The Non-Individual Defendants failed to consider or implement any measure of security that provided protection for the privacy of information about student athletes including by failing to consider or have multiple authentication credentials, background checks, peer reviews, or oversight.

60. These failures allowed Weiss to access private, intimate, personal information pertaining to Plaintiff(s) and their peers, all of which was maintained by Keffer, as encouraged and authorized by the University and the Regents, and all of which Plaintiff(s) and other similar to them entrusted to the Non-Individual Defendants.

61. The recklessness and negligence and misconduct of the Regents, the University, and Keffer in these respects enabled Weiss to target female college athletes to obtain their private and sensitive information without authorization, including but not limited to Plaintiff(s).

62. The Non-Individual Defendants knew that Weiss by virtue of his job duties would be at an advantage over others and would be able to access the other private information and privacy interests of the Plaintiff(s) and their peers.

63. Because the Regents, the University, and Keffer failed to undertake any reasonable security measures or background checks of Weiss, he was enabled to brazenly research and target and invade the privacy of various University athletes,

particularly female athletes, nearly all if not all such women were targeted based on their school affiliation, athletic history, and physical characteristics.

64. Because the Regents, the University, and Keffer failed to supervise Weiss, review his conduct, review his credentials, review his work, and left him free to prey on Plaintiff(s) and others, all without reporting what he was doing in furtherance of his duties, Weiss was able to execute his goal of obtaining private photographs and videos of Plaintiff(s) and others that were never intended to be shared with others or be shared beyond Plaintiff(s)' intimate partners, and likewise for other victims situated similar to the Plaintiff(s).

65. As a result of the University's recklessness, the recklessness of the Regents, and the gross negligence of Keffer, Weiss downloaded personal, intimate digital photographs and videos of Plaintiff(s) and others, all of which Plaintiff(s) and others entrusted to the Non-Individual Defendants.

66. Because the Non-Individual Defendants negligently and recklessly failed to exercise any control over Weiss, Weiss, in furtherance of performance of his job duties, was able to successfully target athletes such as Plaintiff(s) and others similar to them and download, obtain, and use their private information, images, and videos.

67. Because the Non-Individual Defendants negligently and recklessly failed to keep tabs or otherwise supervise or monitor Weiss, he was

able to keep notes on individuals whose photographs and videos he wanted, all of which he obtained, and then viewed, and the Non-Individual Defendants' failure to take any reasonable protective measures was so severe that Weiss even kept detailed notes commenting on the bodies and sexual preferences of Plaintiff(s) and their peers as reported in the indictment.

68. The information that the Non-Individual Defendants permitted Weiss to obtain is highly private, secretive, embarrassing when shared without authorization, and humiliating to become public without authorization.

69. Weiss obtained access—without and in excess of authorization—to student athlete databases of more than 100 colleges and universities across the country that were maintained by Keffer including but not limited to those of university athletes like Plaintiff(s) and others because the University and the Regents failed to take any action or even consider the harm Weiss could do, and actually did, as did Keffer.

70. Plaintiff(s) and others continue to face harm because, despite notice from decades of athletic department complaints and abuse, and widely known social media stockpiles of information that beg for safekeeping, Keffer, the Regents and the University have failed again and again to undertake any review of how Plaintiff(s)' private and personal information is stored, maintained, and who might access such information, how they might access the information, and from where they might access the information.

71. The University and the Regents also failed to investigate Keffer, Keffer's protocols, and failed to monitor or establish safeguards for Keffer's work with the students and their private images to ensure they carried out their duties to safeguard and protect the private information entrusted to them.

72. The University and the Regents have also failed to consider or implement ways to prevent exposing students to Weiss.

73. Neither the University nor the Regents have explained or justified why they failed to undertake any review of the contract with Keffer, failed to investigate Keffer, failed to monitor or establish safeguards for Keffer's work with the students and their private images, and otherwise considered what action they should take to not expose students and others to Weiss.

74. Weiss, through the lack of control and enabling from the Non-Individual Defendants, obtained access to databases containing highly sensitive and private information of the Plaintiff(s) and others similar to them.

75. Many if not all of those databases are maintained by Keffer and was entrusted by Plaintiff(s) to be safeguarded.

76. Plaintiff(s) entrusted the University and the Regents to ensure Keffer safeguarded their private information and images.

77. All of the Non-Individual Defendants failed to consider or execute any action that would have been prudent and would have protected Plaintiff(s)' private

information and the private information of others in similar positions from being accessed by Weiss.

78. After gaining access to unsecured databases, Weiss downloaded the personally identifiable information (PII) and medical data of more than 150,000 athletes including Plaintiff(s).

79. Weiss also downloaded passwords that athletes used to access Keffer's computer system to view and update the athletes' data, including that of Plaintiff(s).

80. The athletes' passwords that Weiss downloaded were encrypted, but was poorly encrypted because of recklessness of the Non-Individual Defendants that Weiss while not being monitored or supervised by the Non-Individual Defendants cracked the encryption, assisted by basic research that he did on the internet.

81. Through open-source Weiss conducted additional research on targeted athletes such as Plaintiff(s) and obtained personal information such as their mothers' maiden names, pets, places of birth, and nicknames, all of which they had entrusted to Non-Individual Defendants to keep private and none of which the Non-Individual Defendants actually safeguarded in any reasonable manner.

82. Using the combined information that he obtained from the student athlete databases and his internet research, based on the lack of supervision or monitoring by the Non-Individual Defendants, despite their control over him, Weiss was able to obtain access to the social media, email, and/or cloud storage

accounts of more than 2,000 targeted athletes and others by guessing or resetting their passwords including but not limited to the Plaintiff(s).

83. Once he obtained access to the accounts of targeted athletes, Weiss searched for and downloaded personal, intimate photographs and videos and other information that were not intended to be viewed by others, not publicly shared, including but not limited to Plaintiff(s) and others similar to them.

84. Weiss also obtained access—without authorization—to the social media, email, and/or cloud storage accounts of more than 1,300 additional students and/or alumni from universities and colleges from around the country including but not limited to Plaintiff(s), caused by the reckless disregard for the safety and personal privacy of the victims committed by the Non-Individual Defendants.

85. Once Weiss gained access to the accounts, he would search for and download personal, intimate photographs and videos.

86. The Non-Individual Defendants have long been on notice that this kind of information Weiss accessed was expected to be kept private, would be embarrassing if accessed by third parties, and any breach would cause significant harm. Despite this, they failed to implement appropriate safeguards.

87. The Regents took no reasonable actions to prevent this unauthorized access.

88. The University took no reasonable actions to prevent this unauthorized

access.

89. Keffer took no reasonable actions to prevent this unauthorized access.

90. The Regents have taken no action to remedy the various tortious harms and invasions they permitted to occur.

91. The University has taken no action to remedy the various tortious harms and invasions they permitted to occur.

92. Keffer has taken no action to remedy the various tortious harms and invasions they permitted to occur.

93. In several instances, Weiss exploited vulnerabilities in the Non-individuals' account authentication processes to gain access to the accounts of students or alumni including but not limited to Plaintiff(s).

94. Weiss leveraged his access to these accounts to gain access to other social media, email, and/or cloud storage accounts.

95. The Regents took no action to prevent this unauthorized access.

96. The University took no action to prevent this unauthorized access.

97. Keffer took no action to prevent this unauthorized access.

98. The Non-Individual Defendants have long been on notice, and it is obvious, that the kind of information Weiss accessed would be reasonably expected to be kept private, would be embarrassing if accessed by third parties, and is the kind of data that in the modern world every commercial and governmental actor is expected to take action to safeguard, particularly since the young student athletes

who are dedicated to the University and the Regents entrusted them to keep all such private information and images confidential and free from access by third parties such as Weiss.

99. Despite all such notice and prior instances of breach of trust, the Non-Individual Defendants failed to protect Plaintiff(s)' private information and images, or to study, consider, or undertake any reasonable method to protect the Plaintiff(s)' privacy and the privacy of others.

100. From in and around 2015, to in and around January 2023, Weiss intentionally accessed—without authorization—information, images, and personal private information of Plaintiff(s) and others, including servers from identified and unidentified social media, email, and/or cloud storage providers that the Non-Individual Defendants knew Plaintiff(s) and others expected and entrusted them to protect and that they failed to protect.

101. Weiss obtained digital photographs, videos, and other private information belonging to more than 3,300 individuals including but not limited to Plaintiff(s) in furtherance of his job duties and his misconduct and the misconduct of the Non-Individual Defendants were violations of the Michigan, Pennsylvania, and Maryland state torts of Invasion of Privacy.

102. From in and around May 2021, to in and around January 2023, Weiss, as a result of the reckless lack of protection, monitoring, or supervision from the

Non-Individual Defendants, knowingly transferred, possessed and used, without lawful authority, information, images, and pictures of Plaintiff(s) and others.

103. From in and around January 2015, to in and around October of 2023, Weiss intentionally accessed—as a result of the Non-Individual Defendants’ failure to protect the privacy of Plaintiff(s) and others—computers, networks, and information relating to Plaintiff(s) and others that was private in nature.

104. After compromising the passwords of approximately 150,000 accounts and gaining access to these same accounts because he was unsupervised or unmonitored, Weiss downloaded personally identifiable information (**PII**) and other health protected information and medical data of more than 150,000 athletes in furtherance of his job duties, including but not limited to Plaintiff(s), all in violation of the Maryland, Michigan, and Pennsylvania tort of Invasion of Privacy.

105. Weiss intended to and did obtain information that furthered his ability to reset the passwords for and access—without authorization—of social media, email, and/or cloud storage accounts of individuals like Plaintiff(s) whose information he obtained from Keffer’s systems, all of which were significantly more easily obtained because of the lack of oversight and monitoring from the Non-Individual Defendants, despite notice of the threat therefor.

106. From in and around 2021, to in and around 2023, Weiss intentionally—without and in excess of authorization—accessed servers Keffer operated, because the Non-Individual Defendants failed to supervise or monitor him, and he as a result obtained digital photographs, videos, and other private information of Plaintiff(s) and others, all in furtherance of job duties, including violations of the Michigan state tort of Invasion of Privacy.

107. From in and around 2021, to in and around 2023, Weiss intentionally accessed—without authorization—computers and servers of the University and the Regents and their technology service providers, thereby invading the privacy of Plaintiff(s) and others, from and after the Non- Individual Defendants’ failure to monitor or supervise Weiss, despite the trust that the Plaintiff(s) placed in the University and the Regents.

108. As additional damage, and as a result of the Non-Individual Defendants’ failure to monitor or supervise Weiss, Weiss was able to reset various passwords including Plaintiff(s)’ account, which amounts to various tortious acts, including violations of privacy, and was perpetrated through various social media, email, and/or cloud storage accounts of one or more University alumni and others.

109. Plaintiff(s) have incurred significant monetary and nonmonetary damages as a result of Defendants’ actions, inactions, torts, negligence, recklessness,

and misconduct, and have been so damaged in excess of \$75,000, exclusive of costs, interest, and fees.

**COUNT I – VIOLATION OF THE COMPUTER FRAUD
AND ABUSE ACT – 18 U.S.C. § 1030**

(Defendant Weiss, University, and Regents)

110. Plaintiff(s) incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

111. Weiss violated the Computer Fraud and Abuse Act by accessing without authorization Plaintiff(s)' private information.

112. Weiss did so in connection with his job duties given to him by the University.

113. Weiss violated the Act because he “intentionally accesse[d] a computer without authorization” and/or “exceed[ed] authorized access, and thereby obtain[ed] ...information.” 18 U.S.C. § 1030(a)(2)(C).

114. Under the law, Weiss was an “inside hacker” because he accessed a computer with permission that dealt with Plaintiff(s) as student athletes, however, Weiss in connection with and furtherance of his job duties then exceeded the parameters of authorized access by entering an area of computerized network of information that was off-limits.

115. Weiss's violations were intentional because he knew he was unauthorized and proceeded nevertheless and did so with approval from the University.

116. The University is vicariously liable for his actions because he did so in furtherance of his role as a sports employee of the University's athletic department.

117. The law is clear that the University is vicariously liable for any offenses of its agents.

118. An employer is responsible for the wrongful acts committed by its employees in the course of their employment.

119. Under 18 U.S.C. § 1030(g), Plaintiff(s) may recover damages in this civil action from Weiss and the University along with injunctive relief or other equitable relief.

120. Plaintiff(s) should be awarded all such forms of damages in this case for Weiss's and the University's willful violation that caused great damage, humiliation, distress, and embarrassment to the Plaintiff(s).

COUNT II – VIOLATIONS OF STORED COMMUNICATIONS ACT
U.S.C. § 2701 et seq

(Defendants Weiss, University and Regents)

121. Plaintiff(s) incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

122. The Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, prohibits

the intentional access of web-based cloud storage and media accounts such as those at issue and other accounts hosted by Keffer that did and do, like for Plaintiff(s), contain personal, private, and intimate information about and relating to Plaintiff(s) and others situated similar to Plaintiff(s).

123. Specifically, 18 U.S.C. § 2701(a) states that it is not lawful for any person to:

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

124. Plaintiff(s)' electronic information and communications were in electronic storage and fit directly within the protections of the statute.

125. The information, messages, files, and media were accessed by Weiss without authorization, in connection with his job duties performed for the University.

126. Weiss's access without authorization in connection with his University job duties was intentional and knowingly done.

127. There is no manner in which Plaintiff(s)' private information, messages, files, and media that is at issue could have been obtained without unauthorized access and would not have been obtained without unauthorized access had Weiss not been an employee of the University working in the specific sports capacity for which

the University hired and employed him.

128. Section 2707 of the Stored Communications Act states that a party may bring a civil action for the violation of this statute.

129. It is a strict liability statute.

130. The statute provides that a person aggrieved by a violation of the act may seek appropriate relief including equitable and declaratory relief, actual damages or damages no less than \$1,000, punitive damages, and reasonable attorney's fee[s] and other litigation costs reasonably incurred according to 18 U.S.C. § 2707(b)-(c).

131. The University and Weiss's access to Plaintiff(s)' private, personal, and intimate information, messages, files, and media was in violation of 18 U.S.C. § 2701(a).

132. The University and Weiss knew they did not have authority to access Plaintiff(s)' private, personal, and intimate information, messages, files, and media and accessed it nevertheless.

133. That willful misconduct violated the Stored Communications Act on various occasions.

134. Plaintiff(s) have incurred significant monetary and nonmonetary damages as a result of these violations of the Stored Communications Act, and Plaintiff(s) request to be compensated for their injuries.

135. Under the statute, Plaintiff(s) should be granted the greater of (1) the sum of their actual damages suffered and any profits made by the University and Weiss as a result of the violations or (2) \$1,000 per violation of the Stored Communications Act.

136. Since the violations were willful, the Court should assess punitive damages against Defendants in addition.

137. Plaintiff(s) should be granted reasonable attorney fees and costs as well.

COUNT III – VIOLATION OF TITLE IX, 20 U.S.C. § 1681(A) *Et Seq.*

(Defendants University and Regents)

138. Plaintiff(s) incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

139. Title IX's provides, "No person in the United States shall on the basis of sex, be ... subject to discrimination under any education program or activity receiving Federal financial assistance ..."

140. Plaintiff(s) are each a "person" under the Title IX statutory language.

141. Weiss targeted women in his unwanted invasions of privacy and his misconduct is discrimination on the basis of sex.

142. The University receives federal financial assistance for its education program and is therefore subject to the provisions of Title IX of the Education Act of 1972, 20 U.S.C. § 1681(a), *et seq.*

143. The University is required under Title IX to investigate allegations of sexual harassment.

144. The University was aware of the sensitive nature of the private and personal information of Plaintiff(s) to which Weiss was able to access given his role.

145. The University and Regents acted with deliberate indifference to sexual harassment by:

- a. Failing to protect Plaintiff(s) and others as required by Title IX;
- b. Failing to adequately investigate and address the complaints regarding the deeply sensitive information Plaintiff(s) provided;
- c. Failing to institute corrective measures to prevent Weiss from sexually harassing other students; and
- d. Failing to adequately investigate the other multiple acts of deliberate indifference.

146. The University and the Regents acted with deliberate indifference as their lack of response to the sexual harassment was clearly unreasonable in light of the known circumstances.

147. The University's failure to promptly and appropriately protect, investigate, and remedy and respond to the sexual harassment of women has effectively denied them equal educational opportunities at the University, including

medical care and sports training.

148. At the time the Plaintiff(s) received some medical training services from the University, they did not know the Non-Individual Defendants failed to adequately consider their safety including in their engagement, hire, training, and supervision of Weiss.

149. As a result of the University's and the Regents' deliberate indifference, Plaintiff(s) have suffered loss of educational opportunities and/or benefits.

150. Plaintiff(s) have incurred, and will continue to incur, attorney's fees and costs of litigation.

151. At the time of Defendants' misconduct and wrongful actions and inactions, Plaintiff(s) were unaware, and or with reasonable diligence could not have been aware, of Defendants' institutional failings with respect to their responsibilities under Title IX.

152. The Regents and the University maintained a policy and/or practice of deliberate indifference for the protection of female student athletes.

153. Defendants' policy and/or practice of deliberate indifference to protection against the invasion of privacy for female athletes created a heightened risk of sexual harassment.

154. Defendants had the ability to prevent the privacy invasion and sexual harassment failed to so prevent the invasions of privacy and harassment.

155. Because of the Regents' and the University's policy and/or practice of deliberate indifference, Plaintiff(s) had their privacy invaded and were sexually harassed by Weiss.

156. Plaintiff(s) should be awarded all such forms of damages in this case for Regents' and the University's conduct that caused great damage, humiliation, and embarrassment to Plaintiff(s)the Plaintiff(s).

COUNT IV -- VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C. § 1983

157. Plaintiff(s) incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

158. The due process clause of the 14th Amendment provides that the state may not deprive a person of life, liberty or property without due process of law.

159. The Regents and the University recklessly exposed Plaintiff(s) to a dangerous predator, Weiss, knowing he could cause serious damage by sexually harassing female students, and also by violating their rights to privacy.

160. Plaintiff(s) as female student athletes were foreseeable victims.

161. The invasion of Plaintiff(s)' privacy was foreseeable.

162. The decisions and actions to deprive Plaintiff of a safe campus constituted affirmative acts that caused and/or increased the risk of harm, as well as physical and emotional injury, to Plaintiff(s).

163. The University and the Regents acted in willful disregard for the safety of Plaintiff(s).

164. The decisions and actions to deprive Plaintiff(s) a safe campus constituted affirmative acts that caused and/or increased the risk of harm, as well as physical and emotional injury, to Plaintiff(s).

165. The University and the Regents acted in willful disregard for the safety of Plaintiff(s).

166. Plaintiff(s) should be awarded all such forms of damages in this case for Regents' and the University's conduct that caused great damage, humiliation, and embarrassment to Plaintiff(s).

COUNT V – FAILURE TO TRAIN AND SUPERVISE UNDER 42 U.S.C. § 1983

(Defendants University and Regents)

167. Plaintiff(s) incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

168. The University and the Regents had the ultimate responsibility and authority to train and supervise their employees, agents, and/or representatives including Weiss and all faculty and staff regarding their duties toward students, faculty, staff and visitors.

169. The University and the Regents failed to train and supervise their employees, agents, and/or representatives including all faculty and staff, regarding

the following duties:

- a. Perceive, understand, and prevent inappropriate sexual harassment on campus;
- b. Perceive, report, and prevent inappropriate invasion of privacy on campus;
- c. Provide diligent supervision to and over student athletes and other individuals, including Weiss;
- d. Thoroughly investigate any invasion of privacy by Weiss;
- e. Ensure the safety of all students, faculty, staff, and visitors to UM's campuses premises;
- f. Provide a safe environment for all students, faculty, staff, and visitors to UM's premises free from sexual harassment; and, invasions of privacy;
- g. Properly train faculty and staff to be aware of their individual responsibility for creating and maintaining a safe environment.
- h. The above list of duties is not exhaustive.

170. The University and the Regents failed to adequately train coaches, trainers, medical staff, Weiss, and others regarding the aforementioned duties which led to violations of Plaintiff's rights.

171. The University and the Regents failure to adequately train was the result of Defendants' deliberate indifference toward the well-being of student athletes and others.

172. The University and the Regents failure to adequately train is closely related to or actually caused Plaintiff's injuries.

173. As a result, the University and the Regents deprived Plaintiff of rights secured by the Fourteenth Amendment to the United States Constitution in violation of 42 U.S.C. § 1983.

174. Plaintiff(s) should be awarded all such forms of damages in this case for Regents' and the University's conduct that caused great damage, humiliation, distress, and embarrassment to the Plaintiff(s).

COUNT VI – INVASION OF PRIVACY
INTRUSION UPON SECLUSION

175. Plaintiff(s) incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

176. Plaintiff(s)' personal social media files, videos, and other images were each in electronic storage and were, and should have been kept, private.

177. All of that private and personal information was wrongfully accessed by Weiss.

178. Weiss's actions were not authorized.

179. The information could not have been obtained but for the Non-Individual Defendants' lack of monitoring and supervision.

180. Plaintiff(s) did not authorize any access.

181. Plaintiff(s) are embarrassed, ashamed, humiliated, and mortified that their private information has been accessed by total strangers and third parties.

182. Plaintiff(s)' social media information and image and videos are a private subject matter.

183. Plaintiff(s) had the right to expect that all of their information would remain private.

184. The means Weiss took to obtain the information was objectively unreasonable.

185. Plaintiff(s) have incurred significant monetary and nonmonetary damages as a result of Defendants' actions and request the appropriate damages.

COUNT VII – GROSS NEGLIGENCE AGAINST THE REGENTS, THE UNIVERSITY, AND KEFFER

186. Plaintiff(s) incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

187. Plaintiff(s)' personal social media files, videos, and other images were each in electronic storage and were, and should have been kept, private.

188. All of that private and personal information was wrongfully accessed by Weiss.

189. Weiss's actions were not authorized.

190. The information could not have been obtained but for the Non-Individual Defendants' lack of monitoring and supervision.

191. Plaintiff(s) did not authorize any access to such information, data, and media by Weiss.

192. Plaintiff(s) are embarrassed, ashamed, humiliated, and mortified that their private information has been access by total strangers and third parties.

193. Plaintiff(s)' social media information and image and videos are a private subject matter.

194. Plaintiff(s) had a right to keep all such information private.

195. Plaintiff(s) entrusted the Regents and the University to ensure methods were undertaken to secure, safeguard, and protect against authorized access to their private information.

196. The Regents and the University do not deny that.

197. Keffer was entrusted to keep Plaintiff(s)' private information private.

198. Keffer does not deny that.

199. The Non-Individual Defendants admit that Plaintiff(s) expected each of them to take reasonable measures to maintain the privacy of Plaintiff(s)' private information.

200. Each of the Non-Individual Defendants admits they are sorry for the breaches of trust that the Plaintiff(s) and the other victims have experienced.

201. The Regents breached their duties to Plaintiff(s) by failing to consider, implement, or follow a policy to oversee how or whether the University conducted its operations in a manner that would have in any manner monitored, supervised, and

ensured that retention and employment of Weiss would not result in a breach of the privacy Plaintiff(s) entrusted to the Regents and the University.

202. The Plaintiff(s) entrusted the University to take measures to secure against Weiss's unauthorized access to their private information.

203. The University failed in its executed of the duty entrusted to the University by the Plaintiff(s) by failing to take any action much less consider means by which to prevent the harm caused to Plaintiff(s) and their peers as alleged in this Complaint, including but not limited to the inaction of failing to consider, determine, enact, and implement a policy to monitor, supervise, and oversee Weiss, or ensure more than one witness or person is verifying that such sensitive and personal and private information is kept confidential.

204. The Regents were supposed to, but failed, to establish University policy, including to monitor personnel, including but not limited to Weiss, so that students on the campus are protected their privacy being invaded.

205. The University failed to provide security to Plaintiff(s) and to other student athletes to be able to be treated by athletic professionals who do not invade their privacy.

206. Keffer recklessly failed to ensure media and information of and pertaining to student athletes including but not limited to Plaintiff(s) was safely

provided and stored even after Plaintiff(s) and other similar to them entrusted Keffer to do so.

207. The Regents had an obligation to support Plaintiff(s), and to develop the campus, its operations including student services, and admissions, and financial aid, IT policies and procedures among others, in a way that at least considered having and executing security measures to protect the personal, private, and intimate images and information of the Plaintiff(s) and others similar to them.

208. The Regents breached those duties because they failed to consider or implement any security measures to protect the personal, private, and intimate images and information of the Plaintiff(s) and others similar to them.

209. The University had a duty but failed to enact, or implement any security measures to protect the personal, private, and intimate images and information of the Plaintiff(s) and others similar to them.

210. Keffer was reckless by failing to equip its computer systems with security that did not make it easy or otherwise possible for Weiss to use quick, basic, and cheap internet research to invade Plaintiff(s)' privacy.

211. Given the sensitive nature of the Plaintiff(s)' private information, each of the Non-Individual Defendants knew of and, as detailed herein, breached their heightened duties to safeguard and protect Plaintiff(s)' privacy by failing to consider,

enact, and implement security measures, and that recklessness exposed Plaintiff(s), and their intimate images and other information.

212. The Regents' failures and omissions in these respects was so reckless that it shows a substantial lack of concern for injuries to Plaintiff(s)the Plaintiff(s).

213. The University's failures and omissions in these respects was so reckless that it shows a substantial lack of concern for injuries to Plaintiff(s)the Plaintiff(s).

214. Keffer's failures and omissions in these respects was so reckless that it shows a substantial lack of concern for injuries to Plaintiff(s)the Plaintiff(s).

215. Plaintiff(s) have incurred significant monetary and nonmonetary damages as a result of Defendants' actions, and should be awarded damages accordingly.

COUNT VIII – NEGLIGENT HIRING

216. Plaintiff(s) incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

217. Plaintiff(s)' personal social media files, videos, and other images and information were each in electronic storage and were, and should have been kept, private.

218. The University had a duty to be reasonable in its review, selection, and hiring of Weiss.

219. The University was not reasonable in its hiring of Weiss.

220. The University failed to study, review, consider, and reasonably determine if Weiss had the kind of training, character, and respect for students to respect or at least not invade their privacy.

221. Plaintiff's private and personal information was wrongfully accessed by Weiss.

222. Weiss's actions were not authorized.

223. The information could not have been obtained but for the University's failure to consider what training to require to hire someone for the job Weiss had, but for the University's failure to consider what credentials Weiss had, but for the failure to consider Weiss's background or review it, and otherwise fail to learn and establish needed conditions that must be satisfied to hire someone to handle personal and sensitive information, or at least not to abuse the position of trust the Plaintiff(s) placed in the University to prudently hire someone for the job Weiss had.

224. Plaintiff(s) did not authorize any access by Weiss and were not asked if they thought he was fit for the job.

225. Plaintiff(s) are embarrassed, ashamed, humiliated, and mortified that their private information has been access by total strangers and third parties.

226. Plaintiff(s)' social media information and image and videos are a private subject matter.

227. Plaintiff(s) had a right to keep all such information private.

228. Plaintiff(s) entrusted the University to ensure methods were undertaken to secure, safeguard, and protect against authorized access to their private information.

229. The University does not deny that.

230. The University breached their duty to reasonably consider the credentials, training, and conditions Weiss should have had to satisfy.

231. But for that, Plaintiff(s) would not have been harmed.

232. But Plaintiff(s) were harmed.

233. The University's breach of its duty to consider much less ensure Weiss was trained to and would follow security measures to protect the personal, private, and intimate images and information of the Plaintiff(s) and others similar to them has caused harm to Plaintiff(s).

234. Given the sensitive nature of the Plaintiff(s)' private information, the University knew that its hiring of Weiss should be more prudent.

235. The University failed in its duty.

236. Plaintiff(s) were harmed as a result.

237. Plaintiff(s) have incurred significant monetary and nonmonetary damages as a result of Defendants' actions and request the appropriate damages.

COUNT IX – NEGLIGENT TRAINING

238. Plaintiff(s) incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

239. The University had an obligation to train Weiss in a manner that would not subject the students including Plaintiff(s) to Weiss invading their privacy.

240. The University failed consider, study, or enact any policy, procedure, or reasonable standard that would have trained Weiss to understand the sensitivity of the information of the Plaintiff(s) entrusted to him and the University.

241. The University failed consider, study, or enact any policy, procedure, or reasonable standard that would have trained Weiss to understand the damage he would do if he invaded the private information of the Plaintiff(s) and to him and the University.

242. The University of Michigan is a substantial institution and Plaintiff(s) reasonably expected a physician coach to be trained to care about and safeguard their personal and private information.

243. Plaintiff(s) understandably did not expect the University to fail to train Weiss about the highly sensitive nature of his position and leave him to his own devices to violate Plaintiff(s) rights and to embarrass and humiliate them.

244. The University failed to train Weiss and that failure damaged the students including but not limited to Plaintiff(s).

245. The University also had an obligation, but failed, to enact and follow a policy to train Weiss to protect students such as Plaintiff(s) from predators.

246. But for these failures by the University, Plaintiff(s) would not have been damaged and would not have had her social media files, videos, and other images that were stored electronically invaded such that they no longer enjoyed privacy and freedom from viewing by others.

247. Plaintiff(s) have been damaged as a result.

248. Plaintiff(s)' social media information and image and videos are a private subject matter.

249. Plaintiff(s) had a right to keep all such information private.

250. The failures of the University were unreasonable.

251. Plaintiff(s) have incurred significant monetary and nonmonetary damages as a result of Defendants' actions and request the appropriate damages.

COUNT X – NEGLIGENT SUPERVISION

252. Plaintiff(s) incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

253. The University had an obligation to supervise Weiss in a manner that would not subject the students including Plaintiff(s) to Weiss invading their privacy.

254. The University failed consider, study, or enact any policy, procedure, or

reasonable standard that would have supervised and monitored Weiss to understand the sensitivity of the information of the Plaintiff(s) entrusted to him and the University.

255. The University failed consider, study, or enact any policy, procedure, or reasonable standard that would have included more secure or multiple source authorization such that Weiss would not have been able to invade Plaintiff(s)' privacy.

256. The University failed to consider or enact any measure to ensure a single actor such as Weiss, left unsupervised, would be able to invade the private information of the Plaintiff(s).

257. The University of Michigan is a substantial institution and Plaintiff(s) reasonably expected a sports coach to be supervised so as to safeguard their personal and private information.

258. Plaintiff(s) understandably did not expect the University to fail to supervise Weiss about the highly sensitive nature of his position and leave him to his own devices to violate Plaintiff(s) rights and to embarrass and humiliate them.

259. The University failed to supervise Weiss, and that failure damaged the students including but not limited to Plaintiff(s).

260. The University also had an obligation, but failed, to enact and follow a policy to supervise Weiss to protect students such as Plaintiff(s) from predators.

261. But for these failures by the University, Plaintiff(s) would not have been damaged and would not have had her social media files, videos, and other images

that were stored electronically invaded such that they no longer enjoyed privacy and freedom from viewing by others.

262. Plaintiff(s) have been damaged as a result.

263. Plaintiff(s)' social media information and image and videos are a private subject matter.

264. Plaintiff(s) had a right to keep all such information private.

265. The failures of the University were unreasonable.

266. Plaintiff(s) have incurred significant monetary and nonmonetary damages as a result of Defendants' actions and request the appropriate damages.

COUNT XI -- NEGLIGENT ENTRUSTMENT

267. Plaintiff(s) incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

268. Plaintiff(s) entrusted the Regents, the University, and Keffer with her private information, social media, images, and videos.

269. The Non-Individual Defendants are liable at law to Plaintiff(s) if they permit the handling and use of Plaintiff(s)' private personal information to be held and handled in a manner that will cause harm to the Plaintiff(s).

270. The Non-Individual Defendants knew of the sensitivity of the information they were handling and relied heavily on their own methods and procedures for so handling the information and using the information.

271. It was a breach of a reasonable standard for the Non-Individual Defendants to not handle and use the personal and private information of the Plaintiff(s) with more care, attention, and sensitivity so as to safeguard and protect from instruction by Weiss.

272. The Regents, the University, and Keffer accepted Plaintiff(s)' entrustment, profited from the parties' relationship, and failed to safeguard Plaintiff(s)' private information, social media, images, and videos despite the entrustment to them.

273. The Regents, the University, and Keffer had a heightened duty to keep Plaintiff(s)' personal social media files, videos, and other images were electronic communications private.

274. The Regents failed in that duty.

275. The University failed in that duty.

276. Keffer failed in that duty.

277. Plaintiff(s)' information was accessed by Weiss.

278. The Non-Individual Defendants failed to seriously or reasonably consider how to safeguard Plaintiff(s)' information.

279. The Non-Individual Defendants failed to carry out their heightened duty to take actions to safeguard and ensure the privacy of Plaintiff(s)' personal and private information.

280. The Non-Individual Defendants each breached their duties by failing to undertake any expected maintenance, protection, monitoring, and supervision to confirm Plaintiff(s)' personal and private information was safe.

281. But for the Non-Individual Defendants' negligent entrustment, Plaintiff(s) would not have been damaged.

282. Plaintiff(s)' social media information and image and videos are a private subject matter.

283. Plaintiff(s) had a right to keep all such information private.

284. Plaintiff(s) have incurred significant monetary and nonmonetary damages as a result of Defendants' actions and request the appropriate damages.

COUNT XII – NEGLIGENT RETENTION

285. Plaintiff(s) incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

286. Plaintiff(s)' personal social media files, videos, and other images were private.

287. The University has had a history of athletic department invasions on the privacy of student athletes and others.

288. The University had a duty to retain Weiss only if he would not continue that unfortunate history.

289. The University had an obligation to retain Keffer only if it would safeguard Plaintiff(s)' private information.

290. The University was warned historically about threats from outside vendors and third-parties to invade the privacy of student athletes and others.

291. The University was warned historically about the threats from personnel of the leaders of the athletic department that trainers can be threats to the invasion of the privacy of student athletes and others.

292. Despite those warnings, and the experiences of the University and the Regents historically, the Regents and the University hired and retained Weiss and he violated the Plaintiff(s)' privacy and the privacy of others.

293. Despite those warnings, and the experiences of the University and the Regents historically, the Regents and the University hired and retained Keffer and it failed to take any reasonable action to safeguard the Plaintiff(s)' privacy and the privacy of others.

294. The University failed take any action to ensure that Weiss was working in an ethical manner that did not invade the privacy of Plaintiff(s).

295. The University failed to take any action to ensure that Keffer stored Plaintiff(s)'s personal and private information in a manner that would not be accessed by others.

296. But for the failures to retain Weiss and Keffer in a prudent and safe manner, Plaintiff(s) would not have been harmed.

297. Plaintiff(s) had a right to keep all her information private.

298. The lack of review or any legitimate historical basis to retain Keffer and Weiss was objectively unreasonable.

299. Plaintiff(s) have incurred significant monetary and nonmonetary damages as a result of Defendants' actions and request the appropriate damages.

COUNT XIII – TRESPASS TO CHATTELS

300. Plaintiff(s) incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

301. By accessing Plaintiff(s)' personal and private information without authorization, Weiss and the University intentionally and harmfully interfered with, and wrongfully exercised dominion or control over, Plaintiff(s)' private and personal information, images, videos, and social media.

302. The aforementioned accessing, dominion, and control was willful and malicious.

303. Plaintiff(s) have incurred significant monetary and nonmonetary damages as a result of Weiss's and the University's intentional and harmful interference with, and wrongful exercise of dominion or control over, Plaintiff(s)' private and personal information.

304. Plaintiff(s) are entitled to exemplary damages as a result of these intentional and harmful act and interference with, and wrongful exercise of control over, their property.

COUNT XIV – COMMON LAW CONVERSION

305. Plaintiff(s) incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

306. By accessing Plaintiff(s)'s personal and private information, Weiss and the University wrongfully exercised dominion or control over Plaintiff(s)'s property, social media, images, videos, and related media, and that access was in denial of, or inconsistent with, Plaintiff(s)' rights therein.

307. The aforementioned exercise of dominion or control was willful and malicious.

308. Plaintiff(s) have incurred significant monetary and nonmonetary damages as a result of these Defendants wrongfully exercising dominion or control

over Plaintiff(s)' personal and private information all of which was in denial of, or inconsistent with, Plaintiff(s)' rights therein.

309. Plaintiff(s) are entitled to exemplary damages as a result of these Weiss and the University wrongfully exercising dominion or control over Plaintiff(s)' property, in denial of, or inconsistent with, Plaintiff(s)' rights therein.

COUNT XV – VIOLATIONS OF MCL § 600.2919a
(Defendant Weiss)

310. Plaintiff(s) incorporate the allegations set forth above by reference with the same force and effect as if fully repeated.

311. MCL § 600.2919a provides:

(1) A person damaged as a result of either or both of the following may recover 3 times the amount of actual damages sustained, plus costs and reasonable attorney fees:

(a) Another person's stealing or embezzling property or converting property to the other person's own use.

(b) Another person's buying, receiving, possessing, concealing, or aiding in the concealment of stolen, embezzled, or converted property when the person buying, receiving, possessing, concealing, or aiding in the concealment of stolen, embezzled, or converted property knew that the property was stolen, embezzled, or converted.

(2) The remedy provided by this section is in addition to any other right or remedy the person may have at law or otherwise.

312. Plaintiff(s) allege the University and the Regents are vicariously liable for Weiss' violation of possessing, concealing, aiding the concealment of, stealing, and/or embezzling Plaintiff(s)' private and personal information and converting that information, those videos, and those images to those Defendants' own use by using that information for their own purposes.

313. Under MCL § 600.2919a, Plaintiff(s) are entitled to 3 times actual damages, plus costs and reasonable attorney fees.

WHEREFORE, Plaintiff(s) request that the Court enter a judgment encompassing the relief requested above, plus significant compensatory damages exceeding \$75,000.00 together with costs, interest and attorney fees, against Defendants, and such other relief to which they are entitled

Date: April 7, 2025

Respectfully Submitted,

By: /s/ Robert J. Lantzy
ROBERT J. LANTZY (P57013)
SARAH L. GORSKI (P82899)
BUCKFIRE LAW FIRM
Attorneys for Plaintiff
29000 Inkster Rd., Suite 150
Southfield, Michigan 48034
Direct (248) 234-9840
robert@buckfirelaw.com
sarah@buckfirelaw.com
Asst: patti@buckfirelaw.com

**U.S. District Court
Eastern District of Michigan (Detroit)
CIVIL DOCKET FOR CASE #: 2:25-cv-10951-MAG-EAS**

****CASE CLOSED ALL ENTRIES MUST BE MADE IN 25-cv-10806.**** Doe v. Board of Regents of the University of Michigan et al

Assigned to: District Judge Mark A. Goldsmith
Referred to: Magistrate Judge Elizabeth A. Stafford
Cause: 28:1345 Property Damage

Date Filed: 04/02/2025
Date Terminated: 05/23/2025
Jury Demand: Plaintiff
Nature of Suit: 370 Other Fraud
Jurisdiction: Federal Question

Plaintiff

Jane Doe

represented by **James Gerard Stranch , IV**
Stranch, Jennings & Garvey, PLLC
223 Rosa L. Parks Avenue
Freedom Building
Ste 200
Nashville, TN 37203
615-254-8801
Fax: 615-250-3937
Email: gstranch@stranchlaw.com
ATTORNEY TO BE NOTICED

Nathan J. Fink
Fink Bressack PLLC
38500 Woodward Avenue
Ste 350
Bloomfield Hills, MI 48304
248-971-2500
Email: nfink@finkbressack.com
ATTORNEY TO BE NOTICED

Yana A. Hart
Clarkson Law Firm
22525 Pacific Coast Highway
Malibu, CA 90265
213-788-4050
Email: yhart@clarksonlawfirm.com
ATTORNEY TO BE NOTICED

David H. Fink
Fink Bressack PLLC
38500 Woodward Ave.
Suite 350
Bloomfield Hills, MI 48304
248-971-2500
Fax: 248-971-2600
Email: dfink@finkbressack.com
ATTORNEY TO BE NOTICED

V.

Defendant

**Board of Regents of the University of
Michigan**

represented by **Daniel B. Tukel**
Butzel Long
201 West Big Beaver Road
Suite 1200
Troy, MI 48084
313-225-7047
Email: tukel@butzel.com
ATTORNEY TO BE NOTICED

Sheldon H. Klein
Butzel
201 West Big Beaver Road
Suite 1200
Troy, MI 48084
248-258-1414
Fax: 248-258-1439
Email: klein@butzel.com
ATTORNEY TO BE NOTICED

Defendant

Keffer Development Services, LLC

represented by **Carl Andrew Fejko**
Dillon McCandless King Coulter Graham
Civil Practice
128 West Cunningham St.
Butler, PA 16001
724-822-2148
Email: cfejko@dmkcg.com
ATTORNEY TO BE NOTICED

Jordan P. Shuber
Dillon McCandless King Coulter &
Graham, LLP
128 West Cunningham Street
Butler, PA 16001
724-283-2200
Fax: 724-283-2298
Email: jshuber@dmkcg.com
ATTORNEY TO BE NOTICED

Thomas W. King , III
Dillon McCandless King Coulter & Graham
LLP
128 West Cunningham Street
Buter, PA 16001
724-283-2200
Email: tking@dmkcg.com
ATTORNEY TO BE NOTICED

Defendant

Matthew Weiss

Date Filed	#	Docket Text
04/02/2025	<u>1</u>	COMPLAINT filed by Jane Doe against Board of Regents of the University of Michigan, Keffer Development Services, LLC, Matthew Weiss with Jury Demand. Plaintiff requests summons issued. Receipt No: AMIEDC-10182743 - Fee: \$ 405. County of 1st Plaintiff: Out of State - County Where Action Arose: Washtenaw - County of 1st Defendant: Washtenaw. [Previously dismissed case: No] [Possible companion case(s): Eastern District of Michigan, 2:25-cv-10806-MAG-DRG, Judge Mark A. Goldsmith] (Fink, David) (Entered: 04/02/2025)
04/03/2025		A United States Magistrate Judge of this Court is available to conduct all proceedings in this civil action in accordance with 28 U.S.C. 636c and FRCP 73. The Notice, Consent, and Reference of a Civil Action to a Magistrate Judge form is available for download at http://www.mied.uscourts.gov (JBro) (Entered: 04/03/2025)
04/03/2025	<u>2</u>	SUMMONS Issued for *Board of Regents of the University of Michigan* (JBro) (Entered: 04/03/2025)
04/03/2025	<u>3</u>	SUMMONS Issued for *Keffer Development Services, LLC* (JBro) (Entered: 04/03/2025)
04/03/2025	<u>4</u>	SUMMONS Issued for *Matthew Weiss* (JBro) (Entered: 04/03/2025)
04/03/2025	<u>5</u>	NOTICE of Appearance by Nathan J. Fink on behalf of Jane Doe. (Fink, Nathan) (Entered: 04/03/2025)
04/04/2025	<u>6</u>	ORDER REASSIGNING CASE from District Judge Matthew F. Leitman to District Judge Mark A. Goldsmith. (NAhm) (Entered: 04/04/2025)
04/04/2025	<u>7</u>	NOTICE of Appearance by Daniel B. Tukel on behalf of Board of Regents of the University of Michigan. (Tukel, Daniel) (Entered: 04/04/2025)
04/07/2025	<u>8</u>	STIPULATED ORDER EXTENDING TIME TO RESPOND TO COMPLAINT UNTIL JUNE 5, 2025 - Signed by District Judge Mark A. Goldsmith. (CCie) (Entered: 04/07/2025)
04/10/2025	<u>9</u>	ORDER OF RECUSAL AND REASSIGNING CASE from Magistrate Judge David R. Grand to Magistrate Judge Elizabeth A. Stafford. (NAhm) (Entered: 04/10/2025)
04/15/2025	<u>10</u>	NOTICE of Appearance by Sheldon H. Klein on behalf of Board of Regents of the University of Michigan. (Klein, Sheldon) (Entered: 04/15/2025)
04/15/2025	<u>11</u>	NOTICE by Jane Doe from 10806 (Attachments: # <u>1</u> Exhibit) (Stinar, Parker) (Entered: 04/15/2025)
04/16/2025	<u>12</u>	NOTICE by Board of Regents of the University of Michigan <i>of filing Motion to Consolidate in case 25-cv-10806</i> (Tukel, Daniel) (Entered: 04/16/2025)
04/16/2025	<u>13</u>	NOTICE of Appearance by James Gerard Stranch, IV on behalf of Jane Doe. (Stranch, James) (Entered: 04/16/2025)
04/22/2025	<u>14</u>	WAIVER OF SERVICE Returned Executed. Keffer Development Services, LLC waiver sent on 4/17/2025, answer due 6/16/2025. (Fink, David) (Entered: 04/22/2025)
04/22/2025	<u>15</u>	ORDER Regarding Status Conference. Signed by District Judge Mark A. Goldsmith. (HRya) (Entered: 04/22/2025)
04/22/2025	<u>16</u>	NOTICE TO APPEAR REMOTELY: Status Conference set for 5/14/2025 at 9:00 AM before District Judge Mark A. Goldsmith. (HRya) (Entered: 04/22/2025)

04/23/2025	17	NOTICE by All Plaintiffs <i>of Filing Motion for Staus Conference</i> (Thompson, Jason) (Entered: 04/23/2025)
04/24/2025	18	NOTICE by Jane Doe from 10806 <i>Majority Plaintiffs' Amended Motion</i> (Stinar, Parker) (Entered: 04/24/2025)
05/06/2025	19	NOTICE by All Plaintiffs re 17 Notice (Other) <i>Corrected Notice of Filing Motion for Status Conference</i> (Thompson, Jason) (Entered: 05/06/2025)
05/14/2025	20	NOTICE of Appearance by Thomas W. King, III on behalf of Keffer Development Services, LLC. (King, Thomas) (Entered: 05/14/2025)
05/14/2025		Minute Entry for remote proceedings before District Judge Mark A. Goldsmith: Status Conference held on 5/14/2025. (Court Reporter: None Present, Not on the Record) (JHea) (Entered: 05/14/2025)
05/14/2025	21	NOTICE of Appearance by Carl Andrew Fejko on behalf of Keffer Development Services, LLC. (Fejko, Carl) (Entered: 05/14/2025)
05/15/2025	22	NOTICE of Appearance by Jordan P. Shuber on behalf of Keffer Development Services, LLC. (Shuber, Jordan) (Entered: 05/15/2025)
05/16/2025	23	NOTICE by Jane Doe <i>re: Supplemental Memorandum in Support of Plaintiff Counsels Motion for Appointment of Interim Class Counsel</i> (Attachments: # 1 Exhibit A) (Hart, Yana) (Entered: 05/16/2025)
05/23/2025	24	ORDER FOR CONSOLIDATION AND RELATED MATTERS. Signed by District Judge Mark A. Goldsmith. (JHea) (Entered: 05/23/2025)
05/23/2025	25	Notice to Parties Regarding Consolidated Case: Order of consolidation entered on *5/23/2025*. Designated lead case number is *25-10806*. (JHea) (Entered: 05/23/2025)

PACER Service Center			
Transaction Receipt			
06/05/2025 16:30:49			
PACER Login:	ThomaKingtking	Client Code:	
Description:	Docket Report	Search Criteria:	2:25-cv-10951-MAG-EAS
Billable Pages:	3	Cost:	0.30

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN**

JANE DOE on behalf of herself and	:	
others similarly situated,	:	Case No.
	:	
Plaintiff,	:	
	:	
v.	:	
	:	
THE UNIVERSITY OF MICHIGAN	:	
BOARD OF REGENTS, KEFFER	:	
DEVELOPMENT SERVICES, LLC,	:	
and MATTHEW WEISS.	:	
	:	
Defendants.	:	

CLASS ACTION COMPLAINT AND JURY DEMAND

INTRODUCTION

1. Plaintiff and the class are current and former student athletes and victims of the data breach on the University of Michigan and Keffer Development Services' databases, exposing their highly sensitive personally identifiable information and medical records to a sexual predator, Matthew Weiss. The breach continued for nearly a decade because the University and Keffer failed to prevent, detect, or stop Weiss from accessing those databases without authorization, allowing him to download the private sensitive information belonging to 150,000 student athletes from over 100 colleges and universities.

2. With that information, Weiss then targeted individual athletes' personal accounts and built dossiers on thousands of young women, downloading their private photos and making notes on their bodies and sexual preferences.

3. This egregious and devastating breach was entirely preventable by the University and Keffer. As noted in a criminal complaint by the United States Attorney in the Eastern District of Michigan, Weiss breached the University and Keffer's systems using *only* compromised credentials belonging to University employees. This is because, on information and belief, neither the University nor Keffer required that its employees implement safeguards like multi-factor authentication to access accounts, a standard practice for all entities collecting personally identifiable information, especially medical information. Nor did the University or Keffer implement reasonable security measures to ensure that only authorized individuals could access student PHI.

4. HIPAA and Michigan state law require entities collecting medical information to secure it using reasonable means. Indeed, the University and Keffer recognized those duties under their policies, with Keffer representing that it uses "industry-standard physical, technical and administrative safeguards to secure data against foreseeable risks, such as unauthorized use, access, disclosure, destruction

or modification.”¹ But despite that promise, Keffer never implemented adequate safeguards, leaving students’ PHI an unguarded target for predators like Weiss.

5. The University and Keffer thus violated their duties to the student athletes under tort, contract, and statutory law, rendering them liable to Plaintiff and the class for the harm this devastating invasion of privacy caused.

PARTIES

6. Plaintiff Jane Doe is a former student athlete at the University of Michigan, and citizen of Texas, where she intends to remain.

7. Defendant, the Regents of the University of Michigan (“the University”), is the entity that governs the University of Michigan. Mich. Comp. Laws §§ 390.3 and 390.4.

8. Defendant, Keffer Development Services, LLC, is a technology vendor operating the electronic medical record system known as “The Athletic Trainer System.” Keffer is headquartered in Grove City, Pennsylvania, and continuously does business in Michigan, as described below, availing it of the protections of Michigan state law. Keffer is a domestic LLC in Pennsylvania.

9. Defendant, Matthew Weiss, is an individual and citizen of Michigan.

¹ https://www.athletictrainersystem.com/pdf_Files/ATS_Privacy_Policy.pdf.

JURISDICTION & VENUE

10. This Court has subject matter jurisdiction under 28 USC § 1332(d) because this is a class action in which the amount in controversy exceeds \$5,000,000, there are more than 100 class members, and the majority of class members are citizens of different states than defendants.

11. This Court also has jurisdiction under 28 USC §§ 1331 and 1367 because Plaintiff alleges a claim under the Stored Communications Act, 18 U.S.C. § 2701(a) et seq., and supplemental jurisdiction over additional related claims under 28 U.S.C. § 1367(a).

12. Plaintiff is also timely filing a Notice of Intent to File Claims in the Court of Claims under MCL 600.6431.

BACKGROUND

Keffer Development Services

13. Keffer is a software vendor that developed the electronic medical record system known as The Athletic Trainer System or “ATS.”

14. The ATS program is designed to store the “protected health information” belonging to students, including their treatment histories, diagnoses, injuries, photos, and personal details, like height and weight.

15. Keffer's operations span the country, including at the University and over 100 colleges and universities. In total, Keffer has collected the PHI belonging to over 150,000 college athletes at those institutions.

16. In collecting this information, Keffer knows it has an obligation to protect it under state and federal law.

17. Its internal policies recognize this obligation:

Keffer Development Services, LLC Privacy Policy

Last updated: July 2, 2024

Keffer Development Services, LLC. ("KDS") is committed to maintaining the security and privacy of

personal information collected through this website, www.atsusers.com (the "Website"), the KDS electronic health record (the "EMR") and the various KDS portals (the "Athlete Portals"). This Privacy Policy discloses KDS' information collection and dissemination practices in connection with the Website, the EMR and the Athlete Portals and applies solely to the information that we collect through those means. This Privacy Policy does not address personal information that you provide to us in other contexts (e.g., through another relationship not expressly described in this Privacy Policy).

Security

KDS understands that storing our data in a secure manner is essential. KDS stores PII, PHI and other data using industry-standard physical, technical and administrative safeguards to secure data against foreseeable risks, such as unauthorized use, access, disclosure, destruction or modification. Please note, however, that while KDS has endeavored to create a secure and reliable website for users, the confidentiality of any communication or material transmitted to/from the Website or via e-mail cannot be guaranteed.

18. Despite recognizing these obligations, Keffer failed to implement basic, industry standard systems to protect students' PHI.

19. As one example, while Keffer maintained the option to incorporate multi-factor authentication to access its ATS applications, on information and belief, it did not *require* that institutions and users do so. That security failure proved critical, as Weiss gained access to student PHI with only the access credentials belonging to other administrators and users.

20. Keffer also lacked any effective data auditing program to measure the download activity from its system, which would have allowed it to detect the massive, years-long breach at issue here.

The University of Michigan

21. The University is an elite-level state institution enrolling students from across the country, including in its athletics programs.

22. In so doing, the University provides its student athletes medical treatment, including from athletic trainers employed by the University.

23. To facilitate that treatment, the University contracted with Keffer to use the ATS application over web and mobile devices.

24. When collecting that information, the University, like Keffer, accepted an obligation to protect it under contract and statutory principles, including under HIPAA.

25. The University, in turn, recognizes the obligation to protect that information under University policy:



How We Secure Your Information

The U-M recognizes the importance of maintaining the security of the information it collects and maintains, and we endeavor to protect information from unauthorized access and damage. The U-M strives to ensure reasonable security measures are in place, including physical, administrative, and technical safeguards to protect your personal information.

26. However, like Keffer, the University failed to implement the security measures needed to fulfill that promise, including staff training on securing credentials, requiring MFA to use the ATS system, and monitoring and auditing access to student files.

27. Nor did the University ensure Keffer had adequate security measures in place to protect its students' PHI from theft and misuse.

28. Indeed, the University lacked adequate training programs to detect and stop breaches like those caused by Weiss.

29. The University and Keffer breached their duties, allowing Weiss to steal the medical and personal records belonging to thousands of students, including sensitive photos and treatment information.

30. Because Keffer and the University failed to implement basic, industry standard security measures, they allowed a predator, ex-football coach Matthew Weiss, to access University students' most sensitive information for nearly a decade.

31. From 2015 to 2023, Weiss gained access to student files within the ATS app using only the access credentials belonging to around 150 ATS users and

University staff. That included elevated levels of access, such as the accounts of trainers and athletic directors.

32. That level of access through that number of accounts is an egregious failing of data security on its face, as no institution with reasonable data security would allow such a breach over an eight-year period.

33. That access allowed Weiss to download the PHI and personal information belonging to over 150,000 student athletes from over 100 institutions, including the University.

34. On information and belief, the compromised information impacted every University student athlete whose information was saved in the ATS program.

35. From there, Weiss furthered his hack by downloading student athletes' passwords to access the system, using those passwords to breach their personal accounts and download personal, intimate photographs and videos that were not publicly shared.

36. If the University had reasonable cybersecurity measures in place to monitor to monitor the activity on its information systems, it would have caught Weiss' malicious activity.

37. In addition, using information derived from the ATS system, Weiss also breached the social media, email, and/or cloud storage accounts of more than 1,300

additional students and/or alumni from universities and colleges from around the country.

38. The University took no reasonable actions to prevent this access despite its duties to its current and former students.

39. Further, the University also failed to investigate the matter as required under state and federal law. Under Title IX, the University must investigate all instances of sexual harassment against students, including invasions of their privacy on the basis of sex.

40. Weiss preyed on and targeted women during his eight-year breach on the basis of their sex. By failing to protect Plaintiff's PHI, inform her of the extent of the invasion, and take all action necessary under Title IX, the University violated its provisions.

41. To this day, and although the University knew about the breach as early as January 2023, the University has not formally informed class members impacted by Weiss's predation and misconduct.

Plaintiff's Allegations

42. Plaintiff is a former student athlete at the University, having attended the University from 2016 to 2020. While in school, Plaintiff was a member of the swim team while Weiss' breach of the University and Keffer's systems was ongoing.

43. As a University swimmer, Plaintiff received treatment from the University's athletic trainer staff, requiring her to disclose information about her treatment, including height, weight, injuries, treatment plans, and analysis on performance and recovery. Indeed, the PHI includes Plaintiffs' x-rays, appointment details, doctor's notes, and other highly sensitive information that Plaintiff would not have shared had she known the University and Keffer would not protect it.

44. That information was saved by the University and Keffer on Keffer's ATS system.

45. Because the University and Keffer never implemented the security safeguards needed to protect student PHI, Weiss compromised the PHI belonging to every University student whose information was saved in Keffer's ATS database, including, on information and belief, Plaintiff's PHI.

46. This breach of information invaded Plaintiff's privacy and has devastated her personally and emotionally, as her highly sensitive PHI was stolen by a predator under circumstances the University never should have allowed to exist.

CLASS ALLEGATIONS

47. Plaintiff brings this lawsuit individually and as a class action on behalf of all others similarly situated pursuant to Rule 23.

48. This action satisfies the numerosity, commonality, predominance, typicality and adequacy factors under Rule 23.

49. The Class is defined as:

All individuals whose personal information was accessed and downloaded by Weiss without authorization.

50. **Numerosity.** The class size is estimated to be over 150,000 current and former students from institutions across the country, including the University. That number renders individual joinder impractical.

51. **Commonality and Predominance.** Class members share common factual and legal questions, including whether:

- a. Whether Keffer and the University had duties to safeguard students' information from theft and unauthorized access;
- b. Whether Keffer and the University breached their duties under state and federal law in failing to protect the Class's personal information;
- c. Whether the University was negligent in training and supervising staff in proper data security;
- d. Whether the University was negligent in supervising and monitoring Weiss;
- e. Whether Keffer and the University took reasonable steps to remediate the effects of the data breach;
- f. Whether the breach injured Plaintiff and the Class;

g. Whether Plaintiff and the Class are entitled to damages;

h. Whether this action may be maintained as a class action;

52. All the above questions are common to the class and predominate over any individual questions that may exist.

53. **Adequacy.** Plaintiff will fairly and adequately represent the Class and have retained Counsel experienced and competent in class actions, including data security class actions. Plaintiff and counsel have no conflicts or interests antagonistic to the Class.

54. **Superiority.** This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Class may be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by defendants' actions. It would otherwise be virtually impossible for class members to seek relief on an individual basis.

CAUSES OF ACTION

COUNT ONE—THE COMPUTER FRAUD AND ABUSE ACT (against Weiss and the University)

55. Plaintiff restates all the allegations above as if set forth below.

56. Weiss violated the Computer Fraud and Abuse Act by unlawfully accessing Plaintiff's private information without authorization.

57. He did so in the course of his assigned job responsibilities at the University. Weiss's actions constitute a violation of the Act because he "knowingly accessed a computer without authorization" and/or "exceeded authorized access, thereby obtaining... information." 18 U.S.C. § 1030(a)(2)(C).

58. Under the law, Weiss qualifies as an "inside hacker" since he initially accessed a computer system with legitimate credentials as part of his work with Plaintiff and Class Members in their capacity as student-athletes. However, he then surpassed the scope of his permitted access by entering restricted areas of the digital network.

59. As described above, Weiss's actions were intentional, as he exploited his access and the University's security failures to prey on young women.

60. The University is vicariously liable for his actions because he committed these actions in furtherance of his role as an employee of the University. The University is liable for a completed offenses, including Weiss's.

61. Under 18 U.S.C. § 1030(g), Plaintiff may recover damages in this civil action from Weiss and the University along with injunctive relief or other equitable relief.

62. Plaintiff should be awarded all such forms of damages in this case for Weiss's and the University's willful violation that caused great damage, humiliation, and embarrassment to Plaintiff and the Class.

**COUNT TWO—THE STORED COMMUNICATIONS ACT
(against Weiss and the University)**

63. Plaintiff restates the allegations above as if set forth below.

64. The Stored Communications Act, 18 U.S.C. § 2701 et seq., prohibits the intentional access of web-based cloud storage and media accounts such as those at issue and other accounts hosted by Keffer that did and do, like for Plaintiff, contain personal, private, and intimate information about and relating to Plaintiff and others situated similar to Plaintiff.

65. Any person who intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

66. Plaintiff's electronic information and communications were in electronic storage and fit directly within the protections of the statute. The information, messages, files, and media were accessed by Weiss without authorization, in connection with his job duties performed for the University.

67. Weiss's access without authorization in connection with his University job duties was intentional and knowingly done.

68. Weiss could not have obtained access without his status as an employee of the University working in the capacity of an athletic trainer with access to the ATS system for which the University employed him.

69. Plaintiff may assert a claim under § 2707 of the Stored Communications Act, for which there is strict liability.

70. The statute provides that a person aggrieved by a violation of the act may seek appropriate relief including equitable and declaratory relief, actual damages or damages no less than \$1,000, punitive damages, and reasonable attorney's fee[s] and other litigation costs reasonably incurred according to 18 U.S.C. § 2707(b)-(c).

71. The University's and Weiss's access to Plaintiff's private, personal, and intimate information, messages, files, and media was in violation of 18 U.S.C. § 2701(a).

72. The University and Weiss knew they did not have authority to access Plaintiff's private, personal, and intimate information, messages, files, and media but accessed it nevertheless.

73. Under the statute, Plaintiff and the Class should be granted the greater of (1) the sum of her actual damages suffered and any profits made by the University and Weiss as a result of the violations or (2) \$1,000 per violation of the Stored Communications Act. And because the actions were willful, Plaintiff and the Class should be entitled to punitive damages, attorney fees, and costs.

**COUNT THREE—TITLE IX, 20 U.S.C. § 1681(A)
(against the University)**

74. Plaintiff incorporates the allegations above as if set forth below.

75. Title IX states, “No person in the United States shall on the basis of sex, be ... subject to discrimination under any education program or activity receiving Federal financial assistance ...”

76. The University receives federal financial assistance for its education program and is therefore subject to the provisions of Title IX of the Education Act of 1972, 20 U.S.C. § 1681(a), et seq.

77. Plaintiff is a “person” under the statute.

78. Weiss explicitly targeted and preyed on women when invading their privacy, constituting discrimination on the basis of sex.

79. The University is required under Title IX to investigate allegations of sexual harassment, including Weiss’s misconduct.

80. The University acted with deliberate indifference to Plaintiff’s rights under Title IX by failing to investigate and notify Plaintiff about the incident as required and failing to adequately institute safeguards and protective measures to prevent Weiss from harassing students and invading their privacy.

81. The University’s failure to promptly and appropriately protect, investigate, and remedy and respond to the sexual harassment of women has

effectively denied them equal educational opportunities at the University, including medical care and sports training.

82. At the time the Plaintiff received medical training services from the University, she did not know the University failed to adequately consider her safety including in its engagement, hire, training, and supervision of Weiss.

83. At the time of the University's misconduct and wrongful actions and inactions, Plaintiff was unaware, and or with reasonable diligence could not have been aware, of the University's institutional failings with respect to their responsibilities under Title IX.

84. The University had the ability to prevent the privacy invasion and sexual harassment that harmed Plaintiff and the Class.

85. Plaintiff and the Class should be awarded all such forms of damages in this case that the University's misconduct caused, including damages, humiliation, and embarrassment to Plaintiff and the Class.

**COUNT FOUR—THE CIVIL RIGHTS ACT UNDER 42 U.S.C. § 1983
“STATE CREATED DANGER”
(against the University)**

86. Plaintiff repeats all allegations above as if set forth below.

87. The due process clause of the 14th Amendment provides that the state may not deprive a person of life, liberty or property without due process of law.

88. The University recklessly exposed Plaintiff to a dangerous predator, Weiss, knowing he could cause serious damage by sexually harassing female students, and also by violating their rights to privacy.

89. Plaintiff as a female student athlete was a foreseeable victim.

90. The invasion of Plaintiff's privacy was foreseeable. The decisions and actions to deprive Plaintiff of a safe campus constituted affirmative acts that caused and/or increased the risk of harm, as well as physical and emotional injury, to Plaintiff.

91. The University acted in willful disregard for the safety of Plaintiff. The decisions and actions to deprive Plaintiff a safe campus constituted affirmative acts that caused and/or increased the risk of harm, as well as physical and emotional injury, to Plaintiff.

92. The University acted in willful disregard for the safety of Plaintiff.

93. Plaintiff should be awarded all such forms of damages in this case for the University's conduct that caused great damage, humiliation, and embarrassment to Plaintiff and the Class.

**COUNT FIVE –THE CIVIL RIGHTS ACT UNDER 42 U.S.C. § 1983
“FAILURE TO TRAIN AND SUPERVISE”
(against the University)**

94. Plaintiff repeats all allegations above as if set forth below.

95. The University had the ultimate responsibility and authority to train and supervise its employees, agents, and/or representatives including Weiss and all faculty and staff regarding their duties toward students, faculty, staff and visitors.

96. The University failed to train and supervise its employees, agents, and/or representatives including all faculty and staff, regarding the following duties: Perceive, understand, and prevent inappropriate sexual harassment on campus; Perceive, report, and prevent inappropriate invasion of privacy campus; Provide diligent supervision to and over student athletes and other individuals, including Weiss; Thoroughly investigate any invasion of privacy by Weiss; Ensure the safety of all students, faculty, staff, and visitors to the University's campuses and premises; Provide a safe environment for all students, faculty, staff, and visitors to the University's premises free from sexual harassment; Properly train faculty and staff to be aware of their individual responsibility for creating and maintaining a safe environment.

97. The University failed to adequately train coaches, trainers, medical staff, Weiss, and others regarding the aforementioned duties which led to violations of Plaintiff's rights.

98. The University's failure to adequately train was the result of its deliberate indifference toward the well-being of student athletes.

99. As a result, the University deprived Plaintiff of rights secured by the Fourteenth Amendment to the United States Constitution in violation of 42 U.S.C. § 1983.

100. Plaintiff should be awarded all such forms of damages in this case for the University's conduct that caused great damage, humiliation, and embarrassment to Plaintiff and the Class.

**COUNT SIX—BREACH OF IMPLIED CONTRACT
(against the University and Keffer)**

101. Plaintiff repeats all allegations above as if set forth below.

102. Keffer and the University impliedly promised to safeguard Plaintiff and the Class's sensitive information when collecting it through the ATS program.

103. Those promises include those in Keffer's privacy policy and the University's school policy.

104. Plaintiff would not have provided her information to the University and Keffer had she known it would not adequately protect it.

105. Plaintiff and the Class provided value to Keffer and the University through direct and indirect means, including through their tuition payments, which the University used in part to secure Keffer's services, and the value of their data to University and Keffer.

106. The University and Keffer both broke their promises to protect Plaintiff and the Class's sensitive information when they failed to implement the basic security safeguards needed to fulfill those promises.

107. That breach caused Plaintiff and the Class contract damages, as they have been deprived of the benefit of their bargain.

**COUNT SEVEN—NEGLIGENCE & NEGLIGENCE PER SE
(against Keffer Only)**

108. Plaintiff realleges all previous paragraphs as if fully set forth below.

109. Plaintiff and members of the Class entrusted their PHI to Keffer. Keffer owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PHI in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

110. Keffer owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Keffer's failure to adequately safeguard their PHI in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PHI—just like the breach that ultimately came to pass. Keffer acted with wanton and reckless disregard for the security and confidentiality of Plaintiff and members of the Class's PHI by disclosing and providing access to this information to third parties and by failing to properly

supervise both the way the PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

111. Keffer owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PHI. Keffer also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the breach.

112. Keffer owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Keffer knew or should have known would suffer injury-in-fact from Keffer's inadequate security protocols. Keffer actively sought and obtained Plaintiff's and members of the Class's personal information and PHI.

113. The risk that unauthorized persons would attempt to gain access to the PHI and misuse it was foreseeable. Given that Keffer holds vast amounts of PHI, it was inevitable that unauthorized individuals would attempt to access Keffer's databases containing the PHI.

114. Keffer's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

115. In addition, Keffer owed a duty of care to Plaintiff and the Class under HIPAA. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PHI is properly maintained.

116. The breach here resulted from multiple failures by Keffer to implement adequate security, including:

- a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);
- b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- d. Failing to ensure compliance with HIPAA security standards under 45 C.F.R. § 164.306(a)(4);
- e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only

to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

- f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);
- g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

117. These regulations were intended to protect the Class at issue here, and Keffer's failure to abide by them caused Plaintiff and the Class damages.

COUNT EIGHT—INVASION OF PRIVACY
“Intrusion Upon Seclusion”
(against Weiss)

118. Plaintiff realleges all allegations above as if fully set forth below.

119. Plaintiff and the Class's PHI was stored electronically and were intended to remain private.

120. Indeed, Plaintiff reasonable expected that information would remain private under the University and Keffer's policies.

121. Weiss unlawfully and intentionally accessed this private and personal information, invading on the seclusion and private affairs of Plaintiff.

122. His actions were unauthorized, and the invasion would be highly offensive to any reasonable person.

123. Plaintiff and the Class never granted permission for this access and Weiss's intrusion is a severe violation of their privacy, causing them severe emotional damages.

WHEREFORE, Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

- a. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing their counsel to represent the Class;
- b. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;
- c. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;
- d. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PHI and PII;
- e. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

- f. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;
- g. Awarding attorneys' fees and costs, as allowed by law;
- h. Awarding prejudgment and post-judgment interest, as provided by law;
- i. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and
- j. Granting such other or further relief as may be appropriate under the circumstances.

Dated: April 2, 2025

Respectfully submitted,

/s/ David H. Fink

David H. Fink (P28235)

Nathan J. Fink (P75185)

FINK BRESSACK

38500 Woodward Ave., Suite 3500

Bloomfield Hills, MI 48304

Tel: (248) 971-2500

dfink@finkbressack.com

nfink@finkbressack.com

J. Gerard Stranch, IV

Grayson Wells (application for admission to be submitted)

STRANCH, JENNINGS & GARVEY, PLLC

The Freedom Center

223 Rosa L. Parks Avenue, Suite 200

Nashville, TN 37203

Tel: (615) 254-8801

gstranch@stranchlaw.com

gwells@stranchlaw.com

CLOSED, reassigned

**U.S. District Court
Eastern District of Michigan (Detroit)
CIVIL DOCKET FOR CASE #: 2:25-cv-10876-MAG-EAS**

****CASE CLOSED ALL ENTRIES MUST BE MADE IN 25-cv-10806.**** Doe v. University of Michigan Board of Regents et al
Assigned to: District Judge Mark A. Goldsmith
Referred to: Magistrate Judge Elizabeth A. Stafford
Cause: 28:1345 Property Damage

Date Filed: 03/28/2025
Date Terminated: 05/23/2025
Jury Demand: Plaintiff
Nature of Suit: 370 Other Fraud
Jurisdiction: Federal Question

Plaintiff

Jane Doe

represented by **Nathan J. Fink**
Fink Bressack PLLC
38500 Woodward Avenue
Ste 350
Bloomfield Hills, MI 48304
248-971-2500
Email: nfink@finkbressack.com
ATTORNEY TO BE NOTICED

Yana A. Hart
Clarkson Law Firm
22525 Pacific Coast Highway
Malibu, CA 90265
213-788-4050
Email: yhart@clarksonlawfirm.com
ATTORNEY TO BE NOTICED

David H. Fink
Fink Bressack PLLC
38500 Woodward Ave.
Suite 350
Bloomfield Hills, MI 48304
248-971-2500
Fax: 248-971-2600
Email: dfink@finkbressack.com
ATTORNEY TO BE NOTICED

V.

Defendant

University of Michigan Board of Regents

represented by **Daniel B. Tukel**
Butzel Long
201 West Big Beaver Road
Suite 1200
Troy, MI 48084
313-225-7047
Email: tukel@butzel.com
ATTORNEY TO BE NOTICED

Sheldon H. Klein

Butzel
 201 West Big Beaver Road
 Suite 1200
 Troy, MI 48084
 248-258-1414
 Fax: 248-258-1439
 Email: klein@butzel.com
ATTORNEY TO BE NOTICED

Defendant**Keffer Development Services, LLC**

represented by **Carl Andrew Fejko**
 Dillon McCandless King Coulter Graham
 Civil Practice
 128 West Cunningham St.
 Butler, PA 16001
 724-822-2148
 Email: cfejko@dmkcg.com
ATTORNEY TO BE NOTICED

Jordan P. Shuber

Dillon McCandless King Coulter &
 Graham, LLP
 128 West Cunningham Street
 Butler, PA 16001
 724-283-2200
 Fax: 724-283-2298
 Email: jshuber@dmkcg.com
ATTORNEY TO BE NOTICED

Thomas W. King , III

Dillon McCandless King Coulter & Graham
 LLP
 128 West Cunningham Street
 Buter, PA 16001
 724-283-2200
 Email: tking@dmkcg.com
ATTORNEY TO BE NOTICED

Defendant**Matthew Weiss**

Date Filed	#	Docket Text
03/28/2025	<u>1</u>	COMPLAINT filed by Jane Doe against Board of Regents of the University of Michigan, Keffer Development Services, LLC, Matthew Weiss with Jury Demand. Plaintiff requests summons issued. Receipt No: AMIEDC-10176090 - Fee: \$ 405. County of 1st Plaintiff: Out of State - County Where Action Arose: Washtenaw - County of 1st Defendant: Washtenaw. [Previously dismissed case: No] [Possible companion case(s): Eastern District of Michigan, 2:25-cv-10806-MAG-DRG, Judge Mark A. Goldsmith] (Fink, David) (Entered: 03/28/2025)

03/28/2025	2	SUMMONS Issued for *Keffer Development Services, LLC* (LHam) (Entered: 03/28/2025)
03/28/2025	3	SUMMONS Issued for *University of Michigan Board of Regents* (LHam) (Entered: 03/28/2025)
03/28/2025	4	SUMMONS Issued for *Matthew Weiss* (LHam) (Entered: 03/28/2025)
03/28/2025	5	NOTICE of Appearance by Daniel B. Tukel on behalf of University of Michigan Board of Regents. (Tukel, Daniel) (Entered: 03/28/2025)
04/02/2025	6	CERTIFICATE of Service/Summons Returned Executed. Keffer Development Services, LLC served on 4/2/2025, answer due 4/23/2025. (Fink, David) (Entered: 04/02/2025)
04/03/2025	7	STIPULATED ORDER Extending Time to Respond to Complaint 1 , (Response due by 6/5/2025). Signed by District Judge Denise Page Hood. (LSau) (Entered: 04/03/2025)
04/03/2025	8	ORDER REASSIGNING CASE from District Judge Denise Page Hood and Magistrate Judge Curtis Ivy, Jr to District Judge Mark A. Goldsmith and Magistrate Judge David R. Grand. (NAhm) (Entered: 04/03/2025)
04/03/2025	9	NOTICE of Appearance by Nathan J. Fink on behalf of Jane Doe. (Fink, Nathan) (Entered: 04/03/2025)
04/10/2025	10	ORDER OF RECUSAL AND REASSIGNING CASE from Magistrate Judge David R. Grand to Magistrate Judge Elizabeth A. Stafford. (NAhm) (Entered: 04/10/2025)
04/15/2025	11	NOTICE of Appearance by Sheldon H. Klein on behalf of University of Michigan Board of Regents. (Klein, Sheldon) (Entered: 04/15/2025)
04/15/2025	12	NOTICE by Jane Doe from 10806 (Attachments: # 1 Exhibit) (Stinar, Parker) Modified on 4/16/2025 (LHam).[NOTICE OF MOTION TO CONSOLIDATE WITH CASE 25-10806 AND NOTICE TO APPOINT LEAD COUNSEL] (Entered: 04/15/2025)
04/16/2025	13	NOTICE by University of Michigan Board of Regents <i>of filing Motion to Consolidate in case 25-cv-10806</i> (Tukel, Daniel) (Entered: 04/16/2025)
04/22/2025	14	WAIVER OF SERVICE Returned Executed. Keffer Development Services, LLC waiver sent on 4/17/2025, answer due 6/16/2025. (Fink, David) (Entered: 04/22/2025)
04/22/2025	15	ORDER Regarding Status Conference. Signed by District Judge Mark A. Goldsmith. (HRya) (Entered: 04/22/2025)
04/22/2025	16	NOTICE TO APPEAR REMOTELY: Status Conference set for 5/14/2025 at 9:00 AM before District Judge Mark A. Goldsmith. (HRya) (Entered: 04/22/2025)
04/23/2025	17	NOTICE by All Plaintiffs <i>of Filing Motion for Staus Conference</i> (Thompson, Jason) (Entered: 04/23/2025)
04/24/2025	18	NOTICE by Jane Doe from 10806 <i>Majority Plaintiffs' Amended Motion</i> (Stinar, Parker) (Entered: 04/24/2025)
05/06/2025	19	NOTICE by All Plaintiffs re 17 Notice (Other) <i>Corrected Notice of Filing Motion for Status Conference</i> (Thompson, Jason) (Entered: 05/06/2025)
05/14/2025	20	NOTICE of Appearance by Thomas W. King, III on behalf of Keffer Development Services, LLC. (King, Thomas) (Entered: 05/14/2025)
05/14/2025		Minute Entry for remote proceedings before District Judge Mark A. Goldsmith: Status Conference held on 5/14/2025. (Court Reporter: None Present, Not on the Record) (JHea) (Entered: 05/14/2025)

05/14/2025	21	NOTICE of Appearance by Carl Andrew Fejko on behalf of Keffer Development Services, LLC. (Fejko, Carl) Modified on 5/14/2025 (LHam). [FILER CALLED - CASE NUMBER ON DOCUMENT IS 25-10946 BUT IT IS FOR 25-10876] (Entered: 05/14/2025)
05/15/2025	22	NOTICE of Appearance by Jordan P. Shuber on behalf of Keffer Development Services, LLC. (Shuber, Jordan) (Entered: 05/15/2025)
05/16/2025	23	NOTICE by Jane Doe re: <i>Supplemental Memorandum in Support of Plaintiff Counsels Motion for Appointment of Interim Class Counsel</i> (Attachments: # 1 Exhibit A) (Hart, Yana) (Entered: 05/16/2025)
05/23/2025	24	ORDER FOR CONSOLIDATION AND RELATED MATTERS. Signed by District Judge Mark A. Goldsmith. (JHea) (Entered: 05/23/2025)
05/23/2025	25	Notice to Parties Regarding Consolidated Case: Order of consolidation entered on *5/23/2025*. Designated lead case number is *25-10806*. (JHea) (Entered: 05/23/2025)

PACER Service Center			
Transaction Receipt			
06/05/2025 16:32:10			
PACER Login:	ThomaKingtking	Client Code:	
Description:	Docket Report	Search Criteria:	2:25-cv-10876-MAG-EAS
Billable Pages:	3	Cost:	0.30

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN**

JANE DOE on behalf of herself and others similarly situated,	:	
	:	Case No.
	:	
Plaintiff,	:	
	:	
	:	
v.	:	
	:	
THE UNIVERSITY OF MICHIGAN	:	
BOARD OF REGENTS,	:	
	:	
KEFFER DEVELOPMENT	:	
SERVICES, LLC,	:	
	:	
&		
MATTHEW WEISS.		
Defendants.		

_____ /

CLASS ACTION COMPLAINT AND JURY DEMAND

INTRODUCTION

1. Plaintiff and the class are current and former student athletes and victims of the data breach on the University of Michigan and Keffer Development Services' databases, exposing their highly sensitive personally identifiable information and medical records to a sexual predator, Matthew Weiss. The breach continued for nearly a decade because the University and Keffer failed to prevent, detect, or stop Weiss from accessing those databases without authorization,

allowing him to download the private sensitive information belonging to 150,000 student athletes from over 100 colleges and universities.

2. With that information, Weiss then targeted individual athletes' personal accounts and built dossiers on thousands of young women, downloading their private photos and making notes on their bodies and sexual preferences.

3. This egregious and devastating breach was entirely preventable by the University and Keffer. As noted in a criminal complaint by the United States Attorney in the Eastern District of Michigan, Weiss breached the University and Keffer's systems using *only* compromised credentials belonging to University employees. This is because, on information and belief, neither the University nor Keffer required that its employees implement safeguards like multi-factor authentication to access accounts, a standard practice for all entities collecting personally identifiable information, especially medical information. Nor did the University or Keffer implement reasonable security measures to ensure that only authorized individuals could access student PHI.

4. HIPAA and Michigan state law require entities collecting medical information to secure it using reasonable means. Indeed, the University and Keffer recognized those duties under their policies, with Keffer representing that it uses "industry-standard physical, technical and administrative safeguards to secure data against foreseeable risks, such as unauthorized use, access, disclosure, destruction

or modification.”¹ But despite that promise, Keffer never implemented adequate safeguards, leaving students’ PHI an unguarded target for predators like Weiss.

5. The University and Keffer thus violated their duties to the student athletes under tort, contract, and statutory law, rendering them liable to Plaintiff and the class for the harm this devastating invasion of privacy caused.

PARTIES

6. Plaintiff Jane Doe is a former student athlete at the University of Michigan, and citizen of Oklahoma, where she intends to remain.

7. Defendant, the Regents of the University of Michigan (“the University”), is the entity that governs the University of Michigan. Mich. Comp. Laws §§ 390.3 and 390.4.

8. Defendant, Keffer Development Services, LLC, is a technology vendor operating the electronic medical record system known as “The Athletic Trainer System.” Keffer is headquartered in Grove City, Pennsylvania, and continuously does business in Michigan, as described below, availing it of the protections of Michigan state law. Keffer is a domestic LLC in Pennsylvania.

9. Defendant, Matthew Weiss, is an individual and citizen of Michigan.

¹ https://www.athletictrainersystem.com/pdf_Files/ATS_Privacy_Policy.pdf

JURISDICTION & VENUE

10. This Court has subject matter jurisdiction under 28 USC § 1332(d) because this is a class action in which the amount in controversy exceeds \$5,000,000, there are more than 100 class members, and the majority of class members are citizens of different states than defendants.

11. This Court also has jurisdiction under 28 USC §§ 1331 and 1367 because Plaintiff alleges a claim under the Stored Communications Act, 18 U.S.C. § 2701(a) et seq., and supplemental jurisdiction over additional related claims under 28 U.S.C. § 1367(a).

12. Plaintiff is also timely filing a Notice of Intent to File Claims in the Court of Claims under MCL 600.6431.

BACKGROUND

Keffer Development Services

13. Keffer is a software vendor that developed the electronic medical record system known as The Athletic Trainer System or “ATS.”

14. The ATS program is designed to store the “protected health information” belonging to students, including their treatment histories, diagnoses, injuries, photos, and personal details, like height and weight.

15. Keffer's operations span the country, including at the University and over 100 colleges and universities. In total, Keffer has collected the PHI belonging to over 150,000 college athletes at those institutions.

16. In collecting this information, Keffer knows it has an obligation to protect it under state and federal law.

17. Its internal policies recognize this obligation:

Keffer Development Services, LLC Privacy Policy

Last updated: July 2, 2024

Keffer Development Services, LLC. ("KDS") is committed to maintaining the security and privacy of

personal information collected through this website, www.atsusers.com (the "Website"), the KDS electronic health record (the "EMR") and the various KDS portals (the "Athlete Portals"). This Privacy Policy discloses KDS' information collection and dissemination practices in connection with the Website, the EMR and the Athlete Portals and applies solely to the information that we collect through those means. This Privacy Policy does not address personal information that you provide to us in other contexts (e.g., through another relationship not expressly described in this Privacy Policy).

Security

KDS understands that storing our data in a secure manner is essential. KDS stores PII, PHI and other data using industry-standard physical, technical and administrative safeguards to secure data against foreseeable risks, such as unauthorized use, access, disclosure, destruction or modification. Please note, however, that while KDS has endeavored to create a secure and reliable website for users, the confidentiality of any communication or material transmitted to/from the Website or via e-mail cannot be guaranteed.

18. Despite recognizing these obligations, Keffer failed to implement basic, industry standard systems to protect students' PHI.

19. As one example, while Keffer maintained the option to incorporate multi-factor authentication to access its ATS applications, on information and belief, it did not *require* that institutions and users do so. That security failure proved critical, as Weiss gained access to student PHI with only the access credentials belonging to other administrators and users.

20. Keffer also lacked any effective data auditing program to measure the download activity from its system, which would have allowed it to detect the massive, years-long breach at issue here.

The University of Michigan

21. The University is an elite-level state institution enrolling students from across the country, including in its athletics programs.

22. In so doing, the University provides its student athletes medical treatment, including from athletic trainers employed by the University.

23. To facilitate that treatment, the University contracted with Keffer to use the ATS application over web and mobile devices.

24. When collecting that information, the University, like Keffer, accepted an obligation to protect it under contract and statutory principles, including under HIPAA.

25. The University, in turn, recognizes the obligation to protect that information under University policy:



How We Secure Your Information

The U-M recognizes the importance of maintaining the security of the information it collects and maintains, and we endeavor to protect information from unauthorized access and damage. The U-M strives to ensure reasonable security measures are in place, including physical, administrative, and technical safeguards to protect your personal information.

26. However, like Keffer, the University failed to implement the security measures needed to fulfill that promise, including staff training on securing credentials, requiring MFA to use the ATS system, and monitoring and auditing access to student files.

27. Nor did the University ensure Keffer had adequate security measures in place to protect its students' PHI from theft and misuse.

28. Indeed, the University lacked adequate training programs to detect and stop breaches like those caused by Weiss.

The University and Keffer breach their duties, allowing Weiss to steal the medical and personal records belonging to thousands of students, including sensitive photos and treatment information

29. Because Keffer and the University failed to implement basic, industry standard security measures, they allowed a predator, ex-football coach Matthew Weiss, to access University students' most sensitive information for nearly a decade.

30. From 2015 to 2023, Weiss gained access to student files within the ATS app using only the access credentials belonging to around 150 ATS users and

University staff. That included elevated levels of access, such as the accounts of trainers and athletic directors.

31. That level of access through that number of accounts is an egregious failing of data security on its face, as no institution with reasonable data security would allow such a breach over an eight-year period.

32. That access allowed Weiss to download the PHI and personal information belonging to over 150,000 student athletes from over 100 institutions, including the University.

33. On information and belief, the compromised information impacted every University student athlete whose information was saved in the ATS program.

34. From there, Weiss furthered his hack by downloading student athletes' passwords to access the system, using those passwords to breach their personal accounts and download personal, intimate photographs and videos that were not publicly shared.

35. In addition, using information derived from the ATS system, Weiss also breached the social media, email, and/or cloud storage accounts of more than 1,300 additional students and/or alumni from universities and colleges from around the country.

36. The University took no reasonable actions to prevent this access despite its duties to its current and former students.

37. Further, the University also failed to investigate the matter as required under state and federal law. Under Title IX, the University must investigate all instances of sexual harassment against students, including invasions of their privacy on the basis of sex.

38. Weiss preyed on and targeted women during his eight-year breach on the basis of their sex. By failing to protect Plaintiff's PHI, inform her of the extent of the invasion, and take all action necessary under Title IX, the University violated its provisions.

39. To this day, and although the University knew about the breach as early as January 2023, the University has not formally informed class members impacted by Weiss's predation and misconduct.

Plaintiff's Allegations

40. Plaintiff is a former gymnast at the University, having attended the University from 2013 to 2017. While in school, Plaintiff participated in the gymnastics program while Weiss' breach of the University and Keffer's systems was ongoing.

41. As a University gymnast, Plaintiff received treatment from the University's athletic trainer staff, requiring her to disclose information about her treatment, including height, weight, injuries, treatment plans, and analysis on

performance and recovery. This is highly sensitive information that Plaintiff would not have shared had she known the University and Keffer would not protect it.

42. That information was saved by the University and Keffer on Keffer's ATS system.

43. Because the University and Keffer never implemented the security safeguards needed to protect student PHI, Weiss compromised the PHI belonging to every University student whose information was saved in Keffer's ATS database, including, on information and belief, Plaintiff's PHI.

44. That included all information that was saved in the ATS database, including her treatment information, injury information, height, weight, and other highly sensitive information.

45. This breach of information invaded Plaintiff's privacy and has devastated her personally and emotionally, as her highly sensitive PHI was stolen by a predator under circumstances the University never should have allowed to exist.

CLASS ALLEGATIONS

46. Plaintiff brings this lawsuit individually and as a class action on behalf of all others similarly situated pursuant to Rule 23.

47. This action satisfies the numerosity, commonality, predominance, typicality and adequacy factors under Rule 23.

48. The Class is defined as:

All individuals whose personal information was accessed and downloaded by Weiss without authorization.

49. **Numerosity.** The class size is estimated to be over 150,000 current and former students from institutions across the country, including the University. That number renders individual joinder impractical.

50. **Commonality and Predominance.** Class members share common factual and legal questions, including whether:

- a. Whether Keffer and the University had duties to safeguard students' information from theft and unauthorized access;
- b. Whether Keffer and the University breached their duties under state and federal law in failing to protect the Class's personal information;
- c. Whether the University was negligent in training and supervising staff in proper data security;
- d. Whether the University was negligent in supervising and monitoring Weiss;
- e. Whether Keffer and the University took reasonable steps to remediate the effects of the data breach;
- f. Whether the breach injured Plaintiff and the Class;
- g. Whether Plaintiff and the Class are entitled to damages;
- h. Whether this action may be maintained as a class action;

51. All the above questions are common to the class and predominate over any individual questions that may exist.

52. **Adequacy.** Plaintiff will fairly and adequately represent the Class and have retained Counsel experienced and competent in class actions, including data security class actions. Plaintiff and counsel have no conflicts or interests antagonistic to the Class.

53. **Superiority.** This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Class may be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by defendants' actions. It would otherwise be virtually impossible for class members to seek relief on an individual basis.

CAUSES OF ACTION

COUNT ONE—THE COMPUTER FRAUD AND ABUSE ACT (against Weiss and the University)

54. Plaintiff restates all the allegations above as if set forth below.

55. Weiss violated the Computer Fraud and Abuse Act by unlawfully accessing Plaintiff's private information without authorization.

56. He did so in the course of his assigned job responsibilities at the University. Weiss's actions constitute a violation of the Act because he "knowingly

accessed a computer without authorization” and/or “exceeded authorized access, thereby obtaining... information.” 18 U.S.C. § 1030(a)(2)(C).

57. Under the law, Weiss qualifies as an “inside hacker” since he initially accessed a computer system with legitimate credentials as part of his work with Plaintiff and Class Members in their capacity as student-athletes. However, he then surpassed the scope of his permitted access by entering restricted areas of the digital network.

58. As described above, Weiss’s actions were intentional, as he exploited his access and the University’s security failures to prey on young women.

59. The University is vicariously liable for his actions because he committed these actions in furtherance of his role as an employee of the University. The University is liable for an completed offenses, including Weiss’s.

60. Under 18 U.S.C. § 1030(g), Plaintiff may recover damages in this civil action from Weiss and the University along with injunctive relief or other equitable relief.

61. Plaintiff should be awarded all such forms of damages in this case for Weiss’s and the University’s willful violation that caused great damage, humiliation, and embarrassment to Plaintiff and the Class.

**COUNT TWO—THE STORED COMMUNICATIONS ACT
(against Weiss and the University)**

62. Plaintiff restates the allegations above as if set forth below.

63. The Stored Communications Act, 18 U.S.C. § 2701 et seq., prohibits the intentional access of web-based cloud storage and media accounts such as those at issue and other accounts hosted by Keffer that did and do, like for Plaintiff, contain personal, private, and intimate information about and relating to Plaintiff and others situated similar to Plaintiff.

64. Any person who intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

65. Plaintiff's electronic information and communications were in electronic storage and fit directly within the protections of the statute. The information, messages, files, and media were accessed by Weiss without authorization, in connection with his job duties performed for the University.

66. Weiss's access without authorization in connection with his University job duties was intentional and knowingly done.

67. Weiss could not have obtained access without his status as an employee of the University working in the capacity of an athletic trainer with access to the ATS system for which the University employed him.

68. Plaintiff may assert a claim under § 2707 of the Stored Communications Act, for which there is strict liability.

69. The statute provides that a person aggrieved by a violation of the act may seek appropriate relief including equitable and declaratory relief, actual damages or damages no less than \$1,000, punitive damages, and reasonable attorney's fee[s] and other litigation costs reasonably incurred according to 18 U.S.C. § 2707(b)-(c).

70. The University's and Weiss's access to Plaintiff's private, personal, and intimate information, messages, files, and media was in violation of 18 U.S.C. § 2701(a).

71. The University and Weiss knew they did not have authority to access Plaintiff's private, personal, and intimate information, messages, files, and media but accessed it nevertheless.

72. Under the statute, Plaintiff and the Class should be granted the greater of (1) the sum of her actual damages suffered and any profits made by the University and Weiss as a result of the violations or (2) \$1,000 per violation of the Stored Communications Act. And because the actions were willful, Plaintiff and the Class should be entitled to punitive damages, attorney fees, and costs.

**COUNT THREE—TITLE IX, 20 U.S.C. § 1681(A)
(against the University)**

73. Plaintiff incorporates the allegations above as if set forth below.

74. Title IX states, “No person in the United States shall on the basis of sex, be ... subject to discrimination under any education program or activity receiving Federal financial assistance ...”

75. The University receives federal financial assistance for its education program and is therefore subject to the provisions of Title IX of the Education Act of 1972, 20 U.S.C. § 1681(a), et seq.

76. Plaintiff is a “person” under the statute.

77. Weiss explicitly targeted and preyed on women when invading their privacy, constituting discrimination on the basis of sex.

78. The University is required under Title IX to investigate allegations of sexual harassment, including Weiss’s misconduct.

79. The University acted with deliberate indifference to Plaintiff’s rights under Title IX by failing to investigate and notify Plaintiff about the incident as required and failing to adequately institute safeguards and protective measures to prevent Weiss from harassing students and invading their privacy.

80. The University’s failure to promptly and appropriately protect, investigate, and remedy and respond to the sexual harassment of women has effectively denied them equal educational opportunities at the University, including medical care and sports training.

81. At the time the Plaintiff received medical training services from the University, she did not know the University failed to adequately consider her safety including in its engagement, hire, training, and supervision of Weiss.

82. At the time of the University's misconduct and wrongful actions and inactions, Plaintiff was unaware, and or with reasonable diligence could not have been aware, of the University's institutional failings with respect to their responsibilities under Title IX.

83. The University had the ability to prevent the privacy invasion and sexual harassment that harmed Plaintiff and the Class.

84. Plaintiff and the Class should be awarded all such forms of damages in this case that the University's misconduct caused, including damages, humiliation, and embarrassment to Plaintiff and the Class.

COUNT FOUR—THE CIVIL RIGHTS ACT UNDER 42 U.S.C. § 1983
“STATE CREATED DANGER”
(against the University)

85. Plaintiff repeats all allegations above as if set forth below.

86. The due process clause of the 14th Amendment provides that the state may not deprive a person of life, liberty or property without due process of law.

87. The University recklessly exposed Plaintiff to a dangerous predator, Weiss, knowing he could cause serious damage by sexually harassing female students, and also by violating their rights to privacy.

88. Plaintiff as a female student athlete was a foreseeable victim.

89. The invasion of Plaintiff's privacy was foreseeable. The decisions and actions to deprive Plaintiff of a safe campus constituted affirmative acts that caused and/or increased the risk of harm, as well as physical and emotional injury, to Plaintiff.

90. The University acted in willful disregard for the safety of Plaintiff. The decisions and actions to deprive Plaintiff a safe campus constituted affirmative acts that caused and/or increased the risk of harm, as well as physical and emotional injury, to Plaintiff.

91. The University acted in willful disregard for the safety of Plaintiff.

92. Plaintiff should be awarded all such forms of damages in this case for the University's conduct that caused great damage, humiliation, and embarrassment to Plaintiff and the Class.

**COUNT FIVE –THE CIVIL RIGHTS ACT UNDER 42 U.S.C. § 1983
“FAILURE TO TRAIN AND SUPERVISE”
(against the University)**

93. Plaintiff repeats all allegations above as if set forth below.

94. The University had the ultimate responsibility and authority to train and supervise its employees, agents, and/or representatives including Weiss and all faculty and staff regarding their duties toward students, faculty, staff and visitors.

95. The University failed to train and supervise its employees, agents, and/or representatives including all faculty and staff, regarding the following duties: Perceive, understand, and prevent inappropriate sexual harassment on campus; Perceive, report, and prevent inappropriate invasion of privacy campus; Provide diligent supervision to and over student athletes and other individuals, including Weiss; Thoroughly investigate any invasion of privacy by Weiss; Ensure the safety of all students, faculty, staff, and visitors to the University's campuses and premises; Provide a safe environment for all students, faculty, staff, and visitors to the University's premises free from sexual harassment; Properly train faculty and staff to be aware of their individual responsibility for creating and maintaining a safe environment.

96. The University failed to adequately train coaches, trainers, medical staff, Weiss, and others regarding the aforementioned duties which led to violations of Plaintiff's rights.

97. The University's failure to adequately train was the result of its deliberate indifference toward the well-being of student athletes.

98. As a result, the University deprived Plaintiff of rights secured by the Fourteenth Amendment to the United States Constitution in violation of 42 U.S.C. § 1983.

99. Plaintiff should be awarded all such forms of damages in this case for the University's conduct that caused great damage, humiliation, and embarrassment to Plaintiff and the Class.

COUNT SIX—BREACH OF IMPLIED CONTRACT (against the University and Keffer)

100. Plaintiff repeats all allegations above as if set forth below.

101. Keffer and the University impliedly promised to safeguard Plaintiff and the Class's sensitive information when collecting it through the ATS program.

102. Those promises include those in Keffer’s privacy policy and the University’s school policy.

103. Plaintiff would not have provided her information to the University and Keffer had she known it would not adequately protect it.

104. Plaintiff and the Class provided value to Keffer and the University through direct and indirect means, including through their tuition payments, which the University used in part to secure Keffer's services, and the value of their data to University and Keffer.

105. The University and Keffer both broke their promises to protect Plaintiff and the Class's sensitive information when they failed to implement the basic security safeguards needed to fulfill those promises.

106. That breach caused Plaintiff and the Class contract damages, as they have been deprived of the benefit of their bargain.

**COUNT SEVEN—NEGLIGENCE & NEGLIGENCE PER SE
(against Keffer Only)**

107. Plaintiff realleges all previous paragraphs as if fully set forth below.

108. Plaintiff and members of the Class entrusted their PHI to Keffer. Keffer owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PHI in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

109. Keffer owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Keffer's failure to adequately safeguard their PHI in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PHI—just like the breach that ultimately came to pass. Keffer acted with wanton and reckless disregard for the security and confidentiality of Plaintiff and members of the Class's PHI by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

110. Keffer owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PHI. Keffer also

owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the breach.

111. Keffer owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Keffer knew or should have known would suffer injury-in-fact from Keffer's inadequate security protocols. Keffer actively sought and obtained Plaintiff's and members of the Class's personal information and PHI.

112. The risk that unauthorized persons would attempt to gain access to the PHI and misuse it was foreseeable. Given that Keffer holds vast amounts of PHI, it was inevitable that unauthorized individuals would attempt to access Keffer's databases containing the PHI.

113. Keffer's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

114. In addition, Keffer owed a duty of care to Plaintiff and the Class under HIPAA. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PHI is properly maintained.

115. The breach here resulted from multiple failures by Keffer to implement adequate security, including:

- a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);
- b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- d. Failing to ensure compliance with HIPAA security standards under 45 C.F.R. § 164.306(a)(4);
- e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

116. These regulations were intended to protect the Class at issue here, and Keffer's failure to abide by them caused Plaintiff and the Class damages.

COUNT EIGHT—INVASION OF PRIVACY
“Intrusion Upon Seclusion”
(against Weiss)

117. Plaintiff realleges all allegations above as if fully set forth below.

118. Plaintiff and the Class's PHI was stored electronically and were intended to remain private.

119. Indeed, Plaintiff reasonable expected that information would remain private under the University and Keffer's policies.

120. Weiss unlawfully and intentionally accessed this private and personal information, invading on the seclusion and private affairs of Plaintiff.

121. His actions were unauthorized, and the invasion would be highly offensive to any reasonable person.

122. Plaintiff and the Class never granted permission for this access and Weiss's intrusion is a severe violation of their privacy, causing them severe emotional damages.

WHEREFORE, Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

- a. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing their counsel to represent the Class;
- b. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;
- c. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;
- d. Enjoining Defendant from further deceptive practices and making untrue statements about the data breach and the stolen PHI and PII;
- e. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;
- f. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;
- g. Awarding attorneys' fees and costs, as allowed by law;
- h. Awarding prejudgment and post-judgment interest, as provided by law;
- i. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

- j. Granting such other or further relief as may be appropriate under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: March 28, 2025

Respectfully submitted,

/s/ David H. Fink

David H. Fink (P28235)

Nathan J. Fink (P75185)

FINK BRESSACK

38500 Woodward Ave., Suite 3500

Bloomfield Hills, MI 48304

Telephone: (248) 971-2500

dfink@finkbressack.com

nfink@finkbressack.com

/s/ Raina Borrelli

Raina Borrelli

STRAUSS BORRELLI PLLC

980 N. Michigan Avenue, Suite 1610

Chicago, IL 60611

Telephone: (872) 263-1100

raina@straussborrelli.com

Attorneys for Plaintiff and Proposed Class

CLOSED, reassigned

**U.S. District Court
Eastern District of Michigan (Detroit)
CIVIL DOCKET FOR CASE #: 2:25-cv-10999-MAG-EAS**

****CASE CLOSED ALL ENTRIES MUST BE MADE IN 25-cv-10806.**** Doe v. Board of Regents of the University of Michigan et al

Assigned to: District Judge Mark A. Goldsmith
Referred to: Magistrate Judge Elizabeth A. Stafford
Demand: \$5,000,000
Cause: 28:1332 Diversity-Personal Injury

Date Filed: 04/08/2025
Date Terminated: 05/23/2025
Jury Demand: Plaintiff
Nature of Suit: 360 P.I.: Other
Jurisdiction: Diversity

Plaintiff

Student Doe

on behalf of herself and all others similarly situated

represented by **James Joseph Pizzirusso**
Hausfeld LLP
1200 17th Street, NW
Suite 600
Washington, DC 20036
202-540-7200
Fax: 202-540-7201
Email: jpizzirusso@hausfeld.com
ATTORNEY TO BE NOTICED

Steven M. Nathan

Hausfeld LLP
NYC
33 Whitehall Street
Ste 14th Floor
New York, NY 10004
646-357-1100
Fax: 212-202-4322
Email: snathan@hausfeld.com
ATTORNEY TO BE NOTICED

Yana A. Hart

Clarkson Law Firm
22525 Pacific Coast Highway
Malibu, CA 90265
213-788-4050
Email: yhart@clarksonlawfirm.com
ATTORNEY TO BE NOTICED

Gary M. Klinger

Milberg Coleman Bryson Phillips Grossman
PLLC
227 W. Monroe Street
Suite 2100
Chicago, IL 60606
866-252-0878

Email: gklinger@milberg.com
ATTORNEY TO BE NOTICED

V.

Defendant

**Board of Regents of the University of
Michigan**

represented by **Daniel B. Tukel**
Butzel Long
201 West Big Beaver Road
Suite 1200
Troy, MI 48084
313-225-7047
Email: tukel@butzel.com
ATTORNEY TO BE NOTICED

Sheldon H. Klein
Butzel
201 West Big Beaver Road
Suite 1200
Troy, MI 48084
248-258-1414
Fax: 248-258-1439
Email: klein@butzel.com
ATTORNEY TO BE NOTICED

Defendant

Keffer Development Services, LLC

represented by **Carl Andrew Fejko**
Dillon McCandless King Coulter Graham
Civil Practice
128 West Cunningham St.
Butler, PA 16001
724-822-2148
Email: cfejko@dmkcg.com
ATTORNEY TO BE NOTICED

Jordan P. Shuber
Dillon McCandless King Coulter &
Graham, LLP
128 West Cunningham Street
Butler, PA 16001
724-283-2200
Fax: 724-283-2298
Email: jshuber@dmkcg.com
ATTORNEY TO BE NOTICED

Thomas W. King , III
Dillon McCandless King Coulter & Graham
LLP
128 West Cunningham Street
Buter, PA 16001
724-283-2200
Email: tking@dmkcg.com
ATTORNEY TO BE NOTICED

Defendant**Matthew Weiss**

Date Filed	#	Docket Text
04/08/2025	<u>1</u>	COMPLAINT filed by Student Doe against Board of Regents of the University of Michigan, Keffer Development Services, LLC, Matthew Weiss with Jury Demand. Plaintiff requests summons issued. Receipt No: AMIEDC-10188505 - Fee: \$ 405. County of 1st Plaintiff: Out of State - Arkansas - County Where Action Arose: Washtenaw - County of 1st Defendant: Washtenaw. [Previously dismissed case: No] [Possible companion case(s): Eastern District of Michigan, 2:25-cv-10806-MAG-DRG, Judge Judge Mark A. Goldsmith] (Attachments: # <u>1</u> Exhibit A - Notice of Data Breach Letter, # <u>2</u> Civil Cover Sheet) (Klinger, Gary) (Entered: 04/08/2025)
04/08/2025	<u>2</u>	SUMMONS Issued for *Board of Regents of the University of Michigan* (LHam) (Entered: 04/08/2025)
04/08/2025	<u>3</u>	SUMMONS Issued for *Keffer Development Services, LLC* (LHam) (Entered: 04/08/2025)
04/08/2025	<u>4</u>	SUMMONS Issued for *Matthew Weiss* (LHam) (Entered: 04/08/2025)
04/08/2025		A United States Magistrate Judge of this Court is available to conduct all proceedings in this civil action in accordance with 28 U.S.C. 636c and FRCP 73. The Notice, Consent, and Reference of a Civil Action to a Magistrate Judge form is available for download at http://www.mied.uscourts.gov (LHam) (Entered: 04/08/2025)
04/10/2025	<u>5</u>	MOTION for Leave to Proceed Pseudonymously by Student Doe. (Klinger, Gary) (Entered: 04/10/2025)
04/10/2025	<u>6</u>	NOTICE of Appearance by James Joseph Pizzirusso on behalf of Student Doe. (Pizzirusso, James) (Entered: 04/10/2025)
04/10/2025	<u>7</u>	NOTICE of Appearance by Steven M. Nathan on behalf of Student Doe. (Nathan, Steven) (Entered: 04/10/2025)
04/11/2025	<u>8</u>	NOTICE of Appearance by Daniel B. Tukel on behalf of Board of Regents of the University of Michigan. (Tukel, Daniel) (Entered: 04/11/2025)
04/14/2025	<u>9</u>	ORDER REASSIGNING CASE from District Judge Brandy R. McMillion and Magistrate Judge Curtis Ivy, Jr to District Judge Mark A. Goldsmith and Magistrate Judge Elizabeth A. Stafford. (SSch) (Entered: 04/14/2025)
04/15/2025	<u>10</u>	NOTICE of Appearance by Sheldon H. Klein on behalf of Board of Regents of the University of Michigan. (Klein, Sheldon) (Entered: 04/15/2025)
04/15/2025	<u>11</u>	NOTICE by Jane Doe from 10806 (Attachments: # <u>1</u> Exhibit) (Stinar, Parker) Modified on 4/16/2025 (LHam). [NOTICE OF MOTION TO CONSOLIDATE WITH CASE 25-10806 AND NOTICE TO APPOINT LEAD COUNSEL] (Entered: 04/15/2025)
04/16/2025	<u>12</u>	NOTICE by Board of Regents of the University of Michigan <i>of filing Motion to Consolidate in case 25-cv-10806</i> (Tukel, Daniel) (Entered: 04/16/2025)
04/18/2025	<u>13</u>	WAIVER OF SERVICE Returned Executed. Student Doe waiver sent on 4/16/2025, answer due 6/16/2025. (Nathan, Steven) Modified on 4/18/2025 (LHam).[AS TO KEFFER DEVELOPMENT SERVICES, LLC] (Entered: 04/18/2025)

04/22/2025	14	ORDER Regarding Status Conference. Signed by District Judge Mark A. Goldsmith. (HRya) (Entered: 04/22/2025)
04/22/2025	15	NOTICE TO APPEAR REMOTELY: Status Conference set for 5/14/2025 at 9:00 AM before District Judge Mark A. Goldsmith. (HRya) (Entered: 04/22/2025)
04/23/2025	16	NOTICE by All Plaintiffs of <i>Filing Motion for Staus Conference</i> (Thompson, Jason) (Entered: 04/23/2025)
04/24/2025	17	RESPONSE to 5 MOTION for Leave to Proceed Pseudonymously filed by Board of Regents of the University of Michigan. (Tukel, Daniel) (Entered: 04/24/2025)
04/24/2025	18	NOTICE by Jane Doe from 10806 <i>Majority Plaintiffs' Amended Motion</i> (Stinar, Parker) (Entered: 04/24/2025)
04/30/2025	19	CERTIFICATE of Service/Summons Returned Executed. Matthew Weiss served on 4/16/2025, answer due 5/7/2025. (Klinger, Gary) (Entered: 04/30/2025)
05/06/2025	20	NOTICE by All Plaintiffs re 16 Notice (Other) <i>Corrected Notice of Filing Motion for Status Conference</i> (Thompson, Jason) (Entered: 05/06/2025)
05/14/2025	21	NOTICE of Appearance by Thomas W. King, III on behalf of Keffer Development Services, LLC. (King, Thomas) (Entered: 05/14/2025)
05/14/2025	22	NOTICE of Appearance by Carl Andrew Fejko on behalf of Keffer Development Services, LLC. (Fejko, Carl) (Entered: 05/14/2025)
05/14/2025		Minute Entry for remote proceedings before District Judge Mark A. Goldsmith: Status Conference held on 5/14/2025. (Court Reporter: None Present, Not on the Record) (JHea) (Entered: 05/14/2025)
05/15/2025	23	NOTICE of Appearance by Jordan P. Shuber on behalf of Keffer Development Services, LLC. (Shuber, Jordan) (Entered: 05/15/2025)
05/16/2025	24	NOTICE by Student Doe re: <i>Supplemental Memorandum in Support of Plaintiff Counsels Motion for Appointment of Interim Class Counsel</i> (Attachments: # 1 Exhibit A) (Hart, Yana) (Entered: 05/16/2025)
05/23/2025	25	ORDER FOR CONSOLIDATION AND RELATED MATTERS. Signed by District Judge Mark A. Goldsmith. (JHea) (Entered: 05/23/2025)
05/23/2025	26	Notice to Parties Regarding Consolidated Case: Order of consolidation entered on *5/23/2025*. Designated lead case number is *25-10806*. (JHea) (Entered: 05/23/2025)

PACER Service Center			
Transaction Receipt			
06/05/2025 16:33:08			
PACER Login:	ThomaKingtking	Client Code:	
Description:	Docket Report	Search Criteria:	2:25-cv-10999-MAG-EAS
Billable Pages:	4	Cost:	0.40

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN**

STUDENT DOE, on behalf of herself and all
others similarly situated,

Plaintiff,

v.

THE UNIVERSITY OF MICHIGAN
BOARD OF REGENTS, KEFFER
DEVELOPMENT SERVICES, LLC, and
MATTHEW WEISS,

Defendants.

CASE NO. 2:25-cv-10999

CLASS ACTION COMPLAINT

DEMAND FOR A JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff Student Doe (“Plaintiff”), individually and on behalf of all others similarly situated, brings this consolidated class action complaint against Defendants The University of Michigan Board of Regents (“University of Michigan”), Keefer Development Services, LLC (“Keefer”), and Matthew Weiss (collectively, “Defendants”), and alleges, upon personal knowledge as to her own actions and experiences and her counsels’ investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Student Doe brings this class action against Defendants University of Michigan and Keefer for the failure to properly secure the highly sensitive personally identifiable information (“PII”) and protected health information (“PHI”) of more than 150,000 student athletes, including herself, which was targeted, accessed, and exfiltrated by former University of Michigan quarterback coach and sexual predator Matthew Weiss, over the course of nearly a decade.

2. Between approximately 2015 and January 2023, University of Michigan’s Coach Weiss, gained unauthorized access to student athlete databases of more than 100 colleges and

universities that were maintained by Keffer, a third-party vendor contracted by the University of Michigan.

3. After gaining access to these databases, Defendant Weiss downloaded the PII and PHI of more than 150,000 athletes.

4. Then, using the information that he obtained from the student athlete databases and his own internet research, University of Michigan's Coach Weiss was able to obtain access to the social media, email, and/or cloud storage accounts of more than 2,000 target athletes. Defendant Weiss also illegally obtained access to the social media, email, and/or cloud storage accounts of more than 1,300 additional students and/or alumni from universities across the country. Once Weiss obtained access to these accounts, he downloaded personal, intimate digital photographs and videos that were never intended to be shared beyond intimate partners.

5. University of Michigan's Coach Weiss primarily targeted female college athletes. He researched and targeted these women based on their school affiliation, athletic history, and physical characteristics.

6. Through this scheme, unknown to account holders, Defendant Weiss downloaded personal, intimate digital photographs and videos.

7. The "Data Breach"—the exfiltration of the PII and PHI of over 150,000 students from the athletic databases Keefer maintained, and the targeted exfiltration of intimate, personal, digital photographs and videos of 3,300 students and athletes¹—continued for nearly a decade because the University of Michigan and Keffer failed to prevent, detect, or stop University of Michigan's Coach Weiss from accessing those databases without and in excess of authorization.

¹ These intimate digital photographs and videos, together with the PII and PHI exposed in the Data Breach, are referred to herein as "Private Information."

8. In March 2025, University of Michigan's Coach Weiss was charged in a 24-count indictment alleging 14 counts of unauthorized access to computers and 10 counts of aggravated identity theft, by the U.S. Attorney for the Eastern District of Michigan, for Weiss's perpetration of the Data Breach.

9. This prolific and egregious Data Breach was entirely preventable by the University of Michigan and Keffer. As noted in a criminal complaint filed by the U.S. Attorney in the Eastern District of Michigan, Defendant Weiss breached the University of Michigan's and Keffer's database systems by exploiting passwords and other vulnerabilities in the University of Michigan's and Keffer's systems and authentication processes. On information and belief, neither the University of Michigan nor Keffer required that its employees or students implement safeguards like multi-factor authentication to access accounts, a standard practice for all entities collecting PII, especially medical data and PHI.

10. The Data Breach was a direct result of the University of Michigan's and Keffer's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiff's and Class Members' PII and PHI, and the University of Michigan's failure to reasonably oversee its employees, leaving the most sensitive and personal information of students, like Student Doe, vulnerable to exploitation by malicious predators like Defendant Weiss.

11. Student Doe brings this action on behalf of all persons whose Private Information was compromised as a result of the University of Michigan's and Keffer's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of the University of Michigan's and Keffer's inadequate information security practices; and (iii) effectively secure its network and database systems containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and

incidents.

12. All three Defendants disregarded the rights of Student Doe and Class Members. The University of Michigan and Keefer intentionally, willfully, recklessly, and/or negligently failed to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failed to disclose that they did not have adequately robust computer systems and security practices to safeguard Private Information; failed to take standard and reasonably available steps to prevent the Data Breach; failed to properly train their staff and employees on proper security measures; failed to provide Student Doe and the class prompt notice of the Data Breach; and, in the case of the University of Michigan, failed to reasonably and adequately supervise its employees, including Defendant Weiss.

13. The University of Michigan's and Keefer's conduct amounts to a violation of the duties they owed to Student Doe under common law tort claims and state and federal statutory law, rendering them liable to Student Doe and the class for the harms caused by this egregious and preventable invasion of privacy. Defendant Weiss is equally liable for the harms inflicted on Student Doe and the class by his intentional hacking and exfiltration of their Private Information under tort and statutory law.

14. Student Doe and the class suffered injury as a result of Defendants' conduct. These injuries included: invasion and loss of privacy, loss of dignity, humiliation, embarrassment, and severe emotional distress.

15. Student Doe seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

16. Student Doe seeks remedies including, but not limited to, compensatory damages, nominal damages, punitive damages, and reimbursement of out-of-pocket costs.

17. Student Doe also seeks injunctive and equitable relief to prevent future injury on behalf of herself and the putative class.

PARTIES

18. Plaintiff Student Doe is a resident and citizen of Arkansas and was a student athlete at Grambling State University. On or about March 26, 2025, Student Doe received notice from the United States Department of Justice Victim Notification System that she was identified as a victim or potential victim in the criminal case against University of Michigan's Coach Weiss: *United States v. Defendant(s) Matthew Weiss*.²

19. Defendant University of Michigan is a public research university in Ann Arbor, Michigan. The University was established on August 26, 1817, in Ann Arbor, Michigan. The University of Michigan Board of Regents is the entity that governs the University of Michigan. Mich. Comp. Laws §§ 390.3 and 390.4.

20. Defendant Matthew Weiss is an individual and citizen of Michigan. On March 20, 2025, Defendant Weiss was indicted on 24 counts of unauthorized access to computers and aggravated identity theft by the U.S. Attorney for the Eastern District of Michigan.

21. Defendant, Keffer Development Services, LLC, is a technology vendor operating the electronic medical record system, which contained the PII and PHI of Plaintiff and class members. Keffer is headquartered in Grove City, Pennsylvania.

JURISDICTION AND VENUE

22. The Court has subject-matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000 exclusive of interest and costs; there are more than 100 members in the proposed class;

² Student Doe's Notice of Data Breach, attached herein as Exhibit A.

and at least one member of the class, including Plaintiff, is a citizen of a state different from *any* Defendant.

23. This Court also has jurisdiction under 28 USC §§ 1331 and 1367 because Plaintiff alleges a claim under the Computer Fraud and Abuse Act, Stored Communications Act, 18 U.S.C. § 2701(a) *et seq.*, and 42 U.S.C. § 1983, and supplemental jurisdiction over additional related claims under 28 U.S.C. § 1367(a).

24. The Court has personal jurisdiction over Defendants named in this action because Defendant University of Michigan is located in and created under the laws of the state of Michigan, Defendant Weiss is a citizen of the state of Michigan, and Defendant Keffer directs business at the state of Michigan, conducts substantial business in Michigan, and has availed itself of the protections of Michigan state law. The conduct by Defendant Keffer which gives rise to the claims against Defendant Keffer in this Complaint was directed at and occurred in Michigan.

25. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. Defendant Keffer and its Athletic Trainer System Software

26. Defendant Keffer is a software development vendor that developed an electronic medical record system known as The Athletic Trainer System, which is used by many universities across the United States.³

27. Defendant Keffer was founded in 1994 and currently collaborates with over 600 clients across 48 states and internationally.⁴ More specifically, Defendant Keffer advertises that it

³ https://www.athletictrainersystem.com/pdf_files/Athlete_Info.pdf.

⁴ <https://www.athletictrainersystem.com/CompanyHistory.aspx>

currently serves over 6500 schools, clinics, and other organizations with over 27,000 users and 2 million athletes.⁵ Among the universities served by Keffer are Defendant University of Michigan, and Student Doe’s alma mater, Grambling State University.

28. Keffer represents that its Athletic Trainer System tool was “designed with athletic trainers for athletic trainers,” and is designed to store PII and PHI belonging to students including their treatment histories, diagnoses, injuries, photos, and personal details, like height and weight, mental health information, and demographic data.⁶

29. In Keffer’s FAQ, it boasts that: “Keffer Development hosts all databases in our SSAE-16, SOC II and FedRamp certified data center” and that “Information security is a high priority in our company.”⁷ It further claims that “On top of our Data Center being FedRamp Certified, ATS is also HIPAA and FERPA compliant. We utilize a company called Compliance Helper to ensure we maintain HIPAA and FERPA compliance.”⁸

30. In its Privacy Policy, Keffer acknowledges that it has obligations as a “business associate” under HIPAA: “To the extent that KDS receives or maintains patient medical information in the course of providing the Clinical EMR, that information is secured, used and disclosed only in accordance with KDS’ legal obligations as a ‘business associate’ under HIPAA.”⁹

31. Keffer’s Privacy Policy further states: “KDS [Keffer] understands that storing our data in a secure manner is essential. KDS stores PII, PHI and other data using industry-standard physical, technical and administrative safeguards to secure data against foreseeable risks, such as

⁵ <https://www.athletictrainersystem.com/Default.aspx>

⁶ See <https://www.athletictrainersystem.com/DemoRequest.aspx>

⁷ https://www.athletictrainersystem.com/pdf_Files/ATS_FAQ.pdf

⁸ *Id.*

⁹ https://www.athletictrainersystem.com/pdf_Files/ATS_Privacy_Policy.pdf

unauthorized use, access, disclosure, destruction or modification. Please note, however, that while KDS has endeavored to create a secure and reliable website for users, the confidentiality of any communication or material transmitted to/from the Website or via e-mail cannot be guaranteed.”¹⁰

32. Despite recognizing these obligations, Keffer failed to implement basic, industry standard systems to protect students’—including Student Doe’s—PII and PHI.

33. As one example, while Keffer maintained the option to incorporate two-factor authentication to access its Athletic Trainer System applications, it did not require that institutions and users do so.¹¹ A two-factor basic security measure that requires an additional layer of authentication on top of a login credential, such as a code sent via text message or email—and critically, would have prevented Defendant Weiss from gaining access to student PHI with only the access credentials belonging to other administrators and users.

34. Recent actions by the FTC, underscore the gross negligence and failings of Keffer in failing to configure its Athletic Trainer System to default to two-factor or multi-factor authentication for access to its systems containing PII and PHI. In February 2023, the FTC published an article titled, *Security Principles: Addressing underlying causes of risk in complex systems*. The article highlighted the importance of MFA, stating: “Multi-factor authentication is widely regarded as a critical security practice because it means a compromised password alone is not enough to take over someone’s account.”¹²

35. Additionally, the FTC’s enforcement actions over the past five years further emphasize the critical and fundamental role MFA plays in an effective data security system, where

¹⁰ *Id.*

¹¹ https://www.athletictrainersystem.com/pdf_Files/ATS_FAQ.pdf

¹² <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems>

the FTC has repeatedly obtained MFA as a form of injunctive relief in data security enforcement actions.¹³

36. Keffer also lacked any effective data auditing program to measure the download activity from its system, which would have allowed it to detect the massive, years-long Data Breach of its systems by University of Michigan's Coach Weiss.

B. Defendant University of Michigan and its Grossly Negligent Oversight over Defendant Weiss and Students' Private Information

37. The University of Michigan is an elite-level educational institution, with an NCAA Division I athletic program, enrolling over 900 student athletes across 29 sports.

38. In maintaining its highly regarded athletics department and program, the University of Michigan provides its student athletes with training from its elite and influential athletic coaches and professionals, including Defendant and former University of Michigan Coach Matthew Weiss.

39. The University of Michigan was grossly negligent on two fronts: (1) in its hiring and supervision of alleged sexual predator Defendant Weiss, and (2) in its hiring and oversight over Defendant Keffer and its entrusting of students' PII and PHI in the care of Defendant Keffer.

A. The University of Michigan was Grossly Negligent in its Hiring and Supervision over Defendant Weiss

40. First, in both the hiring and supervising of athletic coaches and professionals, the University of Michigan owes a duty to student athletes generally to ensure they are protected from predation by its employees and athletic staff. Its coaches and athletic staff—including Coach

¹³ *E.g.*, *In re: Equifax* (July 2019), <https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach>; *In re Drizly* (Oct. 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million>; *In re Chegg* (Oct. 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-brings-action-against-ed-tech-provider-chegg-careless-security-exposed-personal-data-millions>.

Weiss—are entrusted to train, develop, and interact with young student athletes from across the country.

41. The University of Michigan was grossly negligent in its hiring of Defendant Matthew Weiss, in 2021, after Defendant Weiss had been targeting and downloading the sensitive and graphic Private Information of student athletes for *six years*.

42. The University of Michigan was also grossly negligent in its oversight of Defendant Weiss, and consciously and recklessly disregarded its duty to safeguard student athletes from alleged sexual predators, as evidenced by its failure to prevent or even detect the Data Breach perpetrated by its athletic coach Defendant Weiss, during the two years of his employ with the University of Michigan.

43. The University of Michigan was grossly negligent in its failure to investigate the Data Breach as required under state and federal law. Under Title IX, the University of Michigan must investigate all instances of sexual harassment against students, including invasions of their privacy on the basis of sex.

44. Defendant and former University of Michigan Coach Weiss preyed on and targeted women athletes during his eight-year Data Breach targeting their Private Information on the basis of their sex. By failing to protect Plaintiff's PII and PHI, inform her of the extent of the invasion, and taking all action necessary under Title IX, the University violated its obligations under Title IX. Indeed, to this day, and although the University of Michigan knew about the breach as early as January 2023, the University of Michigan has not formally informed class members impacted by Defendant and former University of Michigan Coach Weiss's predation and misconduct.

B. The University of Michigan was Negligent in Hiring/Contracting with Defendant Keffer and in Entrusting Student's PII and PHI to Keffer

45. In addition to providing coaching to its student athletes, the University of Michigan

also provides its student athletes medical treatment, including from athletic trainers employed by the University of Michigan.

46. To facilitate that treatment, the University of Michigan contracted with Keffer to use its Athletic Training System application, which required that student athletes provide the University of Michigan and Keffer with sensitive PII and PHI.

47. When collecting that information, the University of Michigan, like Keffer, accepted an obligation to protect it under contract and statutory principles, including as a “business associate” under HIPAA.

48. The University of Michigan recognizes its obligation to safeguard sensitive PII and PHI and represents in its Privacy Statement that: “The U-M recognizes the importance of maintaining the security of the information it collects and maintains, and we endeavor to protect information from unauthorized access and damage. The U-M strives to ensure reasonable security measures are in place, including physical, administrative, and technical safeguards to protect your personal information.”¹⁴

49. Despite this obligation, the University of Michigan failed to implement the security measures needed to fulfill that promise, including staff and employee training on securing credentials, requiring multi- or two-factor authentication to use Keffer’s Athletic Trainer System, overseeing third-party vendors like Keffer, in which the University of Michigan entrusted student’s sensitive PII and PHI, and monitoring and auditing access to student files and Private Information.

50. In other words, the University of Michigan not only failed to ensure it had implemented sufficient security protocols and procedures across its own systems and staff, but also the University of Michigan failed to ensure Keffer had adequate security measures in place to

¹⁴ <https://umich.edu/about/privacy-statement/>

protect its students' PII and PHI from theft and misuse.

51. Indeed, the University of Michigan lacked adequate training programs to detect and stop breaches like those caused by Defendant Weiss.

C. University of Michigan's Former Coach Weiss and the Data Breach

52. Because Keffer and the University of Michigan failed to implement basic, industry standard security measures, and because the University of Michigan was grossly negligent in its hiring and oversight of Defendant Weiss, together these Defendants allowed an alleged predator, ex-football coach Matthew Weiss, to access students', and in particular female student athletes', most sensitive information for nearly a decade.

53. From 2015 to 2023, Weiss gained access to student files within Keffer's Athletic Trainer System application, through compromising the passwords of a limited number of accounts with elevated access, such as the accounts of trainers and athletic directors.

54. That level of access through that number of accounts is an egregious and grossly negligent failing of data security on its face, as no institution with reasonable data security would allow such a breach over an eight-year period.

55. That access allowed Defendant Weiss to download the PII and PHI belonging to over 150,000 student athletes from over 100 institutions, including the University of Michigan and Grambling State University.

56. From there, Defendant Weiss continued his hack by downloading student athletes' passwords to access the system, using those passwords to breach their personal accounts and download personal, intimate photographs and videos that were not publicly shared. Although the athletes' passwords that Weiss downloaded were purportedly encrypted, Defendant Weiss cracked the encryption with basic internet research he conducted.

57. After cracking their passwords, through open-source research—and through information that appeared to be leaked from other data breaches—Defendant Weiss conducted additional research on targeted athletes to obtain personal information such as their mothers’ maiden names, pets, places of birth, and nicknames.

58. Using the combined information that he obtained from the student athlete databases and his internet research, Defendant Weiss was able to obtain access to the social media, email and/or cloud storage accounts of more than 2,000 targeted athletes by guessing or resetting their passwords.

59. Once University of Michigan’s Coach Weiss obtained access to the accounts of targeted athletes, like Student Doe, Weiss searched for and downloaded personal, intimate photographs and videos that were not publicly shared.

60. Defendant Weiss also obtained access—without and in excess of authorization—to the social media, email, and/or cloud storage accounts of more than 1,300 students and/or alumni from universities and colleges from around the country.

61. Once University of Michigan’s Coach Weiss gained access to these accounts, he would search for and download personal, intimate photographs and videos.

62. In at least several instances, Defendant Weiss exploited vulnerabilities in universities’ account authorization processes to gain access to the accounts of students or alumni. Weiss leveraged his access to these accounts to gain access to other social media, email, and/or cloud storage accounts.

63. The University of Michigan took no reasonable actions to oversee and ensure that coaches it hired were not intentionally and maliciously preying on student athletes and students, took no reasonable actions to prevent this access despite its duties to students, and have taken no

reasonable actions to notify or rectify harm to the victims of University of Michigan Coach Weiss's misconduct and predation.

64. To this day, and although the University knew about the breach as early as January 2023, the University has not formally informed Class Members impacted by Weiss's predation and misconduct.

65. These failings amount to gross negligence on the part of the University of Michigan.

D. Student Doe's Allegations

66. Plaintiff Student Doe is a decorated, former women's basketball player at Grambling State University.

67. While in school, Student Doe participated in the basketball program while Defendant Weiss's Data Breach was ongoing.

68. As a student athlete, Student Doe received treatment from her university's athletic trainer staff, requiring her to disclose information about her treatment, including height, weight, injuries, medications, treatment plans, and analysis on performance and recovery. To receive treatment, Student Doe was required to use the Keffer database, and the PII and PHI Student Doe disclosed was saved on Keffer's system.

69. Because Keffer never implemented the security safeguards needed to protect student Doe's PII and PHI, and because the University of Michigan was grossly negligent in its oversight of its former coach, Defendant Weiss, Defendant Weiss compromised the PII and PHI belonging to every student whose information was saved in Keffer's Athletic Trainer System database, including, on information and belief, Plaintiff's.

70. Defendant Weiss compromised all information that was saved in the Athletic

Trainer System database, including Plaintiff's treatment information, injury information, height, weight, and other highly sensitive information.

71. Student Doe received notice dated March 26, 2025 from the U.S. Department of Justice Victim Notification System that she was identified as a potential victim in the federal action against Defendant Weiss, charging him with 24 counts of unauthorized access to computers and aggravated identity theft.¹⁵

72. After receiving notice from the federal government that read: "If you are receiving this notification, it means that information of yours was found in possession of the defendant,"¹⁶ Student Doe felt violated, deeply disturbed, humiliated, embarrassed, and extremely emotionally distressed; and is experiencing physical manifestations of the stress and anxiety caused by this egregious violation of her privacy—symptoms that are further exacerbated by the fact that Student Doe still has little to no information about the Data Breach.

73. This breach of information invaded Plaintiff's privacy and has devastated her personally and emotionally, as her highly sensitive Private Information was stolen by an alleged predator under circumstances that were entirely preventable by Defendant University of Michigan and Defendant Keffer.

**DEFENDANTS KEFFER AND UNIVERSITY OF MICHIGAN
FAILED TO PROPERLY PROTECT PLAINTIFF'S AND CLASS
MEMBERS' PII AND PHI**

74. Defendants Keffer and University of Michigan did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted PII and PHI it was maintaining for Plaintiff and Class Members, causing the exposure of PII and PHI for 150,000

¹⁵ See *Exhibit A*.

¹⁶

students and former students, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for 3,330 students and former students.

75. The FTC promulgated numerous guides which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

76. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.¹⁷ The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.¹⁸

77. The FTC further recommends that companies not maintain PII and PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

78. Defendants Keffer and University of Michigan failed to properly implement basic

¹⁷ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

¹⁸ *Id.*

DEFENDANTS KEFFER AND UNIVERSITY OF MICHIGAN
FAILED TO COMPLY WITH INDUSTRY STANDARDS

84. Defendants Keffer and University of Michigan did not utilize industry standards appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of PII and PHI for approximately 150,000 students and former students, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for 3,330 students and former students.

85. As explained by the FBI, “[p]revention is the most effective defense against cyberattacks] and it is critical to take precautions for protection.”²⁰

86. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of cyberattacks and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no

²⁰ See How to Protect Your Networks from RANSOMWARE, at 3, <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Dec. 20, 2024).

users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common cyberware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.²¹

87. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the Internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different

²¹ *Id.* at 3-4.

domain (e.g., .com instead of .net) . . .

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it....
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic....²²

88. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendants Keffer and University of Michigan could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure Internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

²² See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), <https://www.cisa.gov/news-events/news/protecting-against-ransomware> (last visited Feb. 20, 2025).

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].²³

89. As described above, experts studying cyber security routinely identify medical facilities as being particularly vulnerable to cyberattacks because of the value of the Private Information they collect and maintain.

90. Several best practices have been identified that at a minimum should be implemented by institutions such as Defendants Keffer and University of Michigan, including, but not limited to, the following: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access

²³ See *Human-Operated Ransomware Attacks: A Preventable Disaster* (Mar 5, 2020), <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>.

sensitive data.

91. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

92. Given that Defendants Keffer and University of Michigan were storing the Private Information of 150,000 individuals, Defendants Keffer and University of Michigan could and should have implemented all of the above measures to prevent cyberattacks, along with the two- or multi-factor authentication discussed earlier in this Complaint.

93. The occurrence of the Data Breach indicates that Defendants Keffer and University of Michigan failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of approximately 150,000 students' and former students' PII and PHI, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for 3,330 students and former students.

**DEFENDANTS KEFFER AND UNIVERSITY OF
MICHIGAN FAILED TO PROPERLY PROTECT PII AND PHI**

94. Defendants Keffer and University of Michigan breached their obligations to Student Doe and Class Members and were otherwise grossly negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches, cyber-attacks, hacking incidents, and ransomware attacks;
- b. Failing to adequately protect patients' Private Information;

- c. Failing to properly monitor its own data security systems for existing or prior intrusions;
- d. Failing to test and assess the adequacy of its data security system;
- e. Failing to develop adequate training programs related to the proper handling of emails and email security practices;
- f. Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;
- g. Failing to require a data security system to ensure the confidentiality and integrity of electronic PHI its network created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- h. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- i. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);
- j. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);
- k. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- l. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- m. Failing to ensure that it was compliant with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);
- n. Failing to train all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);
- o. Failing to ensure that the electronic PHI it maintained is unusable, unreadable, or indecipherable to unauthorized individuals, as Defendants had not encrypted the electronic PHI as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” (45 C.F.R. §

164.304 definition of encryption);

- p. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;
- q. Failing to adhere to industry standards for cybersecurity.

95. As the result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendants Keffer and University of Michigan negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

96. Defendant University of Michigan was also grossly negligent in its failure to oversee the data security practices of third-party vendor—Keffer—in which it entrusted the sensitive private information of its students and former students.

97. Defendant University of Michigan was also grossly negligent in its hiring and oversight of Defendant Weiss, who had been perpetrating this invasion of student's privacy for 6 years before he was hired by the University of Michigan to coach its student athletes, and for 2 years of his employment by the University of Michigan where he coached and worked closely with student athletes at the University of Michigan.

98. Accordingly, as outlined below, Plaintiff and Class Members have already been severely harmed by this egregious violation of their privacy by Defendant Weiss.

CLASS ALLEGATIONS

99. Student Doe brings this nationwide class action on behalf of herself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

100. The Class that Student Doe seeks to represent is defined as follows:

All individuals in the United States whose Private Information was actually or potentially accessed or acquired during the Data Breach,

(“Nationwide Class” or “Class”).

101. Excluded from the Class are Defendants’ officers and directors; any entity in which any Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of any Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

102. Numerosity, Fed. R. Civ. P. 23(a)(1): The Class is so numerous that joinder of all members is impracticable. The U.S. Department of Justice has identified hundreds of thousands of individuals whose Private Information may have been improperly accessed in the Data Breach, has already sent preliminary notice to affected individuals, including Plaintiff.

103. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff’s and Class Members’ Private Information;
- b. Whether Defendants Keefer and University of Michigan failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the hacking incident and Data Breach;
- c. Whether Defendants Keefer and University of Michigan data security systems prior to and during the Data Breach complied with applicable data security laws and regulations, *e.g.*, FTC Guidelines, HIPAA, etc.;
- d. Whether Defendants Keefer’s and University of Michigan’s data security systems prior to and during the Data Breach were consistent with industry standards;
- e. Whether Defendants Keefer and University of Michigan owed a duty to Plaintiffs and Class Members to safeguard their Private Information;
- f. Whether Defendants Keefer and University of Michigan breached their duty to Plaintiffs and Class Members to safeguard their Private Information;
- g. Whether Defendant University of Michigan was grossly negligent in its

hiring and supervision of Defendant Weiss;

- h. Whether Defendant University of Michigan was grossly negligent in its oversight of Defendant Keefer;
- i. Whether Defendants Keefer and University of Michigan knew or should have known that their data security systems and monitoring processes were deficient;
- j. Whether Defendants Keefer and University of Michigan owed a duty to provide Plaintiff and Class Members timely notice of the Data Breach, and whether Defendants Keefer and University of Michigan breached that duty to provide timely notice;
- k. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;
- l. Whether Defendants' conduct was negligent or grossly negligent;
- m. Whether Defendant's conduct was *per se* negligent;
- n. Whether Defendants' conduct violated federal laws;
- o. Whether Defendants' conduct violated state laws; and
- p. Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or punitive damages.

104. Common sources of evidence may also be used to demonstrate Defendants' unlawful conduct on a class-wide basis, including, but not limited to, documents and testimony about its data and cybersecurity measures (or lack thereof); testing and other methods that can prove Defendant's data and cybersecurity systems have been or remain inadequate; documents and testimony about the source, cause, and extent of the Data Breach; and documents and testimony about any remedial efforts undertaken as a result of the Data Breach.

105. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach and Defendants' misfeasance.

106. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent

and protect the interests of the Class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Classes and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

107. Predominance, Fed. R. Civ. P. 23 (b)(3). Defendants engaged in a common course of conduct toward Plaintiff and Class Members, in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way and as a result of the same vulnerabilities. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

108. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants Keefer and University of Michigan. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

109. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Members to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

110. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

111. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

112. Unless a class-wide injunction is issued, Defendants may continue in their failure to properly secure the Private Information of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

113. Further, Defendants acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

114. Defendants acted on grounds that apply generally to the Class as a whole, so that Class certification and the corresponding relief sought are appropriate on a Class-wide basis.

115. Finally, all members of the proposed Class are readily ascertainable. The U.S. Department of Justice has identified hundreds of thousands of individuals whose Private Information may have been improperly accessed in the Data Breach and has already sent preliminary notice to affected individuals, including Plaintiff.

CAUSES OF ACTION

FIRST COUNT

Negligence & Negligence *Per Se* Against Keffer Only (On Behalf of Plaintiff and the Nationwide Class)

116. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

117. Plaintiff brings this claim individually and on behalf of Class Members.

118. Plaintiff and Class Members entrusted their PII and PHI to Keffer. Keffer owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PII and PHI in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

119. Plaintiff and Class Members entrusted their Private Information to Keffer on the premise and with the understanding that Defendant Keffer would safeguard their information, use their PII and PHI for purposes that would benefit Plaintiffs and Class Members and/or not disclose their PII and PHI to unauthorized third parties.

120. Defendant Keffer owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Keffer's failure to adequately safeguard their PII and PHI in accordance

with industry standards concerning data security would result in the compromise of that PII and PHI—as occurred in the Data Breach.

121. Defendant Keffer acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' PII and PHI by misrepresenting their commitments to high standards of security in their public representations on their website, when in reality their lack of security allowed Plaintiff's and Class Members' PII and PHI to be accessed and exfiltrated by malicious actors including Defendant Weiss.

122. Defendant Keffer further breached its duty of care to Plaintiff and Class Members by failing to properly supervise both the way the PII and PHI was stored, used, and exchanged, and those in its employ who were responsible for ensuring the reasonable and adequate security of that PII and PHI.

123. Defendant Keffer had full knowledge of the sensitive nature of the PII and PHI and the types of harm that Plaintiff and Class Members could and would suffer if the PII and PHI was wrongfully disclosed.

124. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII and PHI, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendant Keffer's security protocols to ensure that the PII and PHI of Plaintiffs and Class Members in Defendant Keffer's possession was adequately secured and protected.

125. Defendant Keffer had, and continues to have, a duty to timely disclose that Plaintiff's and Class Members' PII and PHI within their possession was compromised and precisely the type(s) of information that were compromised.

126. Defendant Keffer had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII and PHI.

127. Defendant Keffer owed to Plaintiff and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their PII and PHI. Keffer also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the breach.

128. Defendant Keffer owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Keffer knew or should have known would suffer injury-in-fact from Defendant Keffer's inadequate security protocols. Keffer actively sought and obtained Plaintiff's and Class Members' PII and PHI.

129. The risk that unauthorized persons would attempt to gain access to the PII and PHI in Defendant Keffer's care, and misuse it was foreseeable. Given that Defendant Keffer holds vast amounts of PII and PHI, it was inevitable that unauthorized individuals would attempt to access Keffer's databases containing the PII and PHI.

130. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like HIPAA and/or Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

131. These regulations were intended to protect the Class at issue here, and Keffer's failure to abide by them caused Plaintiff and the Class damages.

132. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PHI is

properly maintained.

133. Defendant Keffer's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant Keffer and Class Members, which is recognized by laws and regulations, as well as common law. Defendant Keffer was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach and was considered a "business associate" under HIPAA.

134. In addition, Defendant Keffer had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

135. Defendant Keffer's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII and PHI.

136. Defendant Keffer systematically failed to provide adequate security for data in its possession.

137. Defendant Keffer was subject to an "independent duty," untethered to any contract between Defendant Keffer and Plaintiff or Class Members.

138. The specific negligent acts and omissions committed by Defendant Keffer include, but are not limited to, the following:

- a. Upon information and belief, mishandling emails, so as to allow for unauthorized person(s) to access Plaintiff's and Class Members' PII and PHI;
- b. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's Class Members' PII And PHI, including, but not limited to, its failure to require two- or multi-factor authentication for access to its Athletic Trainer System;

- c. Failing to adequately monitor the security of its networks and systems;
- d. Failure to periodically ensure that their computer systems and networks had plans in place to maintain reasonable data security safeguards and detect an unauthorized access;
- e. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);
- f. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2)
- g. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- h. Failing to ensure compliance with HIPAA security standards under 45 C.F.R. § 164.306(a)(4);
- i. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- j. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1); and
- k. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

139. Defendant Keffer, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII and PHI within Defendant Keffer's possession.

140. Defendant Keffer, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Private Information.

141. Defendant Keffer, through its actions and/or omissions, unlawfully breached its

duty to timely disclose to Plaintiff and Class Members that the PII and PHI within Defendant Keffer's possession might have been compromised and precisely the type of information compromised.

142. It was foreseeable that Defendant Keffer's failure to use reasonable measures to protect Plaintiff and Class Members' PII and PHI would result in injury to Plaintiff and Class Members.

143. It was foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' PII and PHI would result in injuries to Plaintiff and Class Members.

144. Defendant Keffer's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PII and PHI to be compromised.

145. Keffer's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

146. Defendant's breaches of duties caused Plaintiff and Class Members to suffer from identity theft, invasion of privacy, severe emotional distress, loss of dignity, and embarrassment, and other physical and mental harm.

147. As a result of Defendant Keffer's negligence and breaches of duties, Plaintiff and Class Members are in danger of imminent harm in that their PII and PHI, which is still in the possession of third parties, including predator Defendant Weiss, will be used for malicious and deviant purposes.

SECOND COUNT

**Negligent Hiring and Supervision and Gross Negligence Against University of Michigan
Only
(On Behalf of Plaintiff and the Nationwide Class)**

148. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

a. Negligent Supervision over Defendant Keffer

149. At all relevant times, Keffer was the University of Michigan's agent. University of Michigan granted Keffer access to Plaintiff's and Class Members' PII And PHI without properly:

- a. Vetting Keffer;
- b. Inquiring about, investigating, or monitoring Keffer's data security practices;
- c. Training Keffer;
- d. Advising Keffer of the duties owed to Plaintiff and Class Members; or
- e. Advising Keffer of the confidential nature of Plaintiff's and Class Members PII and PHI.

150. The University of Michigan was negligent and failed to exercise care in the hiring, supervision, and retention of Keffer – whose inadequate data security, training, procedures, protocols, and network infrastructure led to the Data Breach and caused the damages suffered by Plaintiff and Class Members, as alleged herein.

151. At all times relevant hereto, University of Michigan owed a duty to Plaintiff and Class Members to train and supervise its agents, vendors, and third parties handling sensitive student data in its possession and control, and to ensure they recognized the duties owed to Plaintiff and Class Members to keep their PII and PHI safe from unauthorized access and disclosure.

152. The University of Michigan owed a duty to Plaintiff and Class Members to ensure Keffer had adequate data security procedures and practices sufficient to protect Plaintiff's and

Class Members' PII and PHI, prior to hiring or contracting with Keffer.

153. After hiring or contracting with Keffer, the University of Michigan also owed a continuing duty to Plaintiff and Class Members to ensure Keffer continued to employ adequate data security procedures and practices to protect Plaintiff's and Class Members' PII and PHI from unauthorized access or disclosure.

154. The University of Michigan was on notice of the importance of data security because of previous highly publicized data breaches affecting HIPAA business associates and PHI.

155. Despite being aware of this risk, University of Michigan failed to ensure that Keffer employed adequate data security measures to protect Plaintiff's and Class Members' PII and PHI from unauthorized disclosure and access by parties with criminal, malicious, and predatory intent.

156. The University of Michigan knew or should have known that its failure to ensure that Keffer employed adequate data security measures would create a foreseeable and unreasonable risk of harm to Plaintiff and Class Members.

157. As a direct and proximate result of the University of Michigan's breach of its duties, and their negligent hiring, training, and supervision of Keffer, Plaintiffs' and Class Members' PII and PHI were compromised and stolen in the Data Breach.

b. Grossly Negligent Hiring and Supervision as to Defendant Weiss

158. Between 2021 and 2023, University of Michigan's Coach Matthew Weiss was the employee and agent of Defendant University of Michigan.

159. The University of Michigan owed a duty of care to Class Members to use reasonable care in hiring and retaining only those employees who would not cause Class Members to suffer injury.

160. During this time, University of Michigan granted Weiss access to Class Members

and to Plaintiff's and Class Members' Private Information without properly:

- a. Vetting Weiss;
- b. Inquiring about, investigating, or monitoring Weiss's data security practices and computer use;
- c. Perceiving, understanding, and preventing inappropriate sexual harassment on campus;
- d. Perceiving, reporting, and preventing inappropriate invasion of privacy campus;
- e. Providing diligent supervision to and over student athletes and other individuals, including Defendant Weiss;
- f. Thoroughly investigating any invasion of privacy by Defendant Weiss;
- g. Ensuring the safety of all students, faculty, staff, and visitors to the University of Michigan's campuses and premises;
- h. Providing a safe environment for all students, faculty, staff, and visitors to the University of Michigan's premises free from sexual harassment; and
- i. Properly training faculty and staff to be aware of their individual responsibility for creating and maintaining a safe environment.

161. The University of Michigan was negligent and failed to exercise care in the hiring, supervision, and retention of Weiss – whose inappropriate, unlawful, and highly invasive and offensive conduct led to the Data Breach and caused the damages suffered by Plaintiff and Class Members, as alleged herein.

162. At all times relevant hereto, University of Michigan owed a duty to Plaintiff and Class Members to train and supervise its agents, employees, and athletic staff and coaches—including Defendant Weiss—while he was in the course of his employment, agency and/or

representation of the University of Michigan and while he interacted with young female students, handled sensitive student data in the University of Michigan's control and possession and control, and was in close proximity to students to ensure they recognized the duties owed to Plaintiff and Class Members to not abuse them.

163. Defendant Weiss's unlawful Data Breach started years before University of Michigan hired Defendant Weiss to serve as a coach to its student athletes, and yet University of Michigan failed to perform a reasonable background check or take other reasonable and adequate pre-hiring precautions to ensure that its employees did not have malicious, criminal, or inappropriate intentions towards students.

164. It was reasonably foreseeable given the *6 years* of Defendant Weiss's hacking and harassment of students and student athletes that preceded his hiring by the University of Michigan that he would continue his unlawful and egregious invasion of students' privacy, unless properly supervised.

165. The University of Michigan failed to investigate, or adequately investigate, or was grossly negligent in investigating Defendant Weiss's background and misconduct towards students and student athletes.

166. The University of Michigan knew or should have known that its failure to ensure that Defendant Weiss did not have malicious, criminal, or inappropriate intentions towards students would cause a foreseeable and unreasonable risk of harm to Plaintiff and Class Members.

167. The University of Michigan knew, or by the exercise of diligence and reasonable care should have known, that Weiss was improperly searching for, accessing, inspecting, downloading, exporting, and stealing Plaintiff's and Class Members Private Information.

168. It was reasonably foreseeable given Defendant Weiss's six-year-long history of

harassing actions toward students and student athletes that he would continue his pattern of abuse of students, including Plaintiff and Class Members, unless properly supervised.

169. The University of Michigan controlled Weiss's coaching, his hours, his company computer and network access, and his authorization for access to Keffer's systems and databases. The University of Michigan had the ability and duty to monitor Weiss's searches, views, downloads, uploads, and other activities involving these systems, databases, and student data. Yet University of Michigan either (a) monitored those activities, yet did nothing to stop them, or (b) willingly chose not to monitor those activities. University of Michigan thus breached its duty reasonably to supervise or monitor its employees and stop any unauthorized inspection or disclosure of confidential and sensitive Private Information and was grossly negligent in so doing.

170. The University of Michigan was grossly negligent in permitting its employees, including Defendant Weiss, to use its computers, computer networks, or credentials to access the Private Information Plaintiff and Class Members.

171. The Data Breach occurred while Defendant Weiss was acting in the course of his employment, agency and/or representation of the University of Michigan.

172. University of Michigan's hiring and supervision over Defendant Weiss was so reckless as to demonstrate a substantial lack of concern for whether injury would result to Plaintiff and Class Members.

173. University of Michigan's hiring and supervision over Defendant Weiss was substantially more than negligent.

174. As a direct and proximate result of the University of Michigan's breach of its duties, and their negligent hiring, training, and supervision of Weiss, Plaintiffs' and Class Members' Private Information was compromised and stolen in the Data Breach.

175. The University of Michigan tolerated, authorized and/or permitted a custom, policy, practice or procedure of insufficient supervision and failed to adequately screen, counsel or discipline Defendant Weiss, with the result that Defendant Weiss was allowed to violate the rights of persons such as Plaintiff and Class Members with impunity.

176. Defendant University of Michigan actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

177. Plaintiff and Class Members are entitled to compensatory, consequential, punitive, and nominal damages suffered as a result of the Data Breach.

THIRD COUNT
Breach of Implied Contract Against Keffer Only
(On Behalf of Plaintiff and the Nationwide Class)

178. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

179. Defendant Keffer, as a condition of providing its services, required Plaintiff and Class Members to provide and entrust their PII and PHI.

180. By Plaintiff and Class Members providing their PII and PHI to Defendant Keffer, and by Defendant Keffer accepting this PII and PHI and representing it would maintain the safety and security of this PII and PHI, including through its privacy policies, the parties mutually assented to implied contracts. These implied contracts included an implicit agreement and understanding that (1) Defendant Keffer would adequately safeguard Plaintiff's and Class Members' PII and PHI from foreseeable threats, (2) that Defendant Keffer would delete the information of Plaintiff and Class Members once it no longer had a legitimate need; and (3) that Defendant Keffer would provide Plaintiff and Class Members with notice within a reasonable

amount of time after suffering a data breach.

181. Defendant Keffer provided consideration by providing its services, while Plaintiff and Class Members provided consideration by paying for its services, either directly or indirectly through their enrollment at educational institutions, and providing valuable property—*i.e.*, their PII and PHI—to Defendant Keffer. Defendant Keffer benefitted from the receipt of this PII and PHI by increased income through providing its Athletic Trainer Software.

182. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant Keffer.

183. Defendant Keffer breached its implied contracts with Plaintiff and Class Members by failing to safeguard and protect their PII and PHI or providing timely and accurate notice to them that their PII and PHI was compromised due to the Data Breach.

184. Defendant Keffer's breaches actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

FOURTH COUNT
Unjust Enrichment against Keffer Only
(On Behalf of Plaintiff and the Nationwide Class)

185. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein

186. Plaintiff pleads this Count in the alternative to her Implied Contract claim.

187. Plaintiff and Class Members conferred a monetary benefit on Defendant Keffer, either directly or indirectly through their educational institutions, by providing Defendant with payment for its services and with valuable PII and PHI in exchange for the use of Keffer's Athletic Trainer System software

188. Defendant Keffer enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and PHI.

189. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant Keffer instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

190. Under the principles of equity and good conscience, Defendant Keffer should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant Keffer failed to implement appropriate data management and security measures that are mandated by industry standards.

191. Defendant Keffer acquired the monetary benefit and PII and PHI through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

192. If Plaintiff and Class Members knew that Defendant Keffer had not secured their PII and PHI, they would not have consented to provide it to Defendant Keffer, either directly or indirectly.

193. Plaintiff and Class Members have no adequate remedy at law.

194. Defendant Keffer actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

195. As a direct and proximate result of Defendant Keffer's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

196. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

FIFTH COUNT
Invasion of Privacy: Intrusion Upon Seclusion
Against Defendant Weiss Only
(On Behalf of Plaintiff and the Nationwide Class)

197. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein

198. Plaintiff and the Class's Private Information was stored electronically and was intended to remain private.

199. Plaintiff and Class Members had a reasonable expectation of privacy in the Private Information Defendant Weiss hacked, accessed, viewed, exfiltrated, and kept detailed personal notes on.

200. Defendant Weiss unlawfully and intentionally accessed this private and personal information, invading on the seclusion and private affairs of Plaintiff and Class Members.

201. Defendant Weiss's actions were unauthorized, and the invasion would be highly offensive to any reasonable person.

202. A reasonable person of ordinary sensibilities would consider the viewing of Plaintiff's and Class Members' Private Information by an unauthorized person to be highly offensive.

203. Plaintiff and the Class never granted permission for this access and Defendant Weiss's intrusion is a severe violation of their privacy, causing them severe emotional damages.

204. Defendant Weiss actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, which injury-in-fact and damages are ongoing,

imminent, immediate, and which they continue to face.

205. Plaintiffs and Class Members are entitled to compensatory, consequential, punitive, and nominal damages suffered as a result of the Data Breach.

SIXTH COUNT
Violation of the Civil Rights Act: Failure to Train and Supervise
Against only the University of Michigan
42 U.S.C. § 1983
(On Behalf of Plaintiff and the Nationwide Class)

206. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

207. The University of Michigan had the ultimate responsibility and authority to train and supervise its employees, agents, and/or representatives including Defendant Weiss and all faculty and staff regarding their duties toward students, faculty, staff and visitors.

208. The University of Michigan failed to train and supervise its employees, agents, and/or representatives including all faculty and staff, regarding the following duties:

- a. Perceiving, understanding, and preventing inappropriate sexual harassment on campus;
- b. Perceiving, reporting, and preventing inappropriate invasion of privacy on campus;
- c. Providing diligent supervision to and over student athletes and other individuals, including Defendant Weiss;
- d. Thoroughly investigating any invasion of privacy by Defendant Weiss;
- e. Ensuring the safety of all students, faculty, staff, and visitors to the University of Michigan's campuses and premises;
- f. Providing a safe environment for all students, faculty, staff, and visitors to the University of Michigan's premises free from sexual harassment; and

- g. Properly training faculty and staff to be aware of their individual responsibility for creating and maintaining a safe environment

209. The University of Michigan failed to adequately train coaches, trainers, medical staff, Weiss, and others regarding the duties listed above which led to violations of Plaintiff's and Class Members' rights

210. The University of Michigan's failure to adequately train was the result of its deliberate indifference toward the well-being of student athletes.

211. As a result, the University of Michigan deprived Plaintiff and Class Members of rights secured by the Fourteenth Amendment to the United States Constitution in violation of 42 U.S.C. § 1983.

212. Defendant University of Michigan actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages—including humiliation, embarrassment, loss of dignity, and severe emotional distress—which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

213. Plaintiff and Class Members are entitled to compensatory, consequential, punitive, and nominal damages suffered as a result of the Data Breach.

SEVENTH COUNT
Violation of the Civil Rights Act: State Created Danger
Against only the University of Michigan
42 U.S.C. § 1983
(On Behalf of Plaintiff and the Nationwide Class)

214. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

215. The due process clause of the 14th Amendment provides that the state may not deprive a person of life, liberty or property without due process of law.

216. The University of Michigan recklessly exposed Plaintiff to a dangerous alleged predator, Defendant Weiss, knowing he could cause serious damage by sexually harassing female students, and also by violating their rights to privacy.

217. In hiring Defendant Weiss, six years into his scheme to invade the privacy of female students, University of Michigan took an affirmative action that increased the risk that Plaintiff and Class Members would be exposed to harm by the misconduct and unlawful acts of Defendant Weiss.

218. In putting Defendant Weiss in a coaching position at the University of Michigan, a position of power with easy access to student athletes and female students, University of Michigan placed Plaintiff and Class Members—all students and student athletes—specifically at risk.

219. The University of Michigan knew or should have known that hiring an alleged sexual predator—Defendant Weiss—would specifically endanger Plaintiff and Class Members.

220. Plaintiff, as a female student athlete was a foreseeable victim.

221. The invasion of Plaintiff's and Class Members privacy was foreseeable. The decisions and actions to deprive Plaintiff and Class Members of a safe educational experience constituted affirmative acts that caused and/or increased the risk of harm, as well as physical and emotional injury, to Plaintiff and Class Members.

222. The University of Michigan acted in willful disregard for the safety of Plaintiff and Class Members, or the University of Michigan was grossly negligent and wantonly reckless in its disregard for the safety of Plaintiff and Class Members.

223. The decisions and actions to deprive Plaintiff and Class Members a safe college experience constituted affirmative acts that caused and/or increased the risk of harm, as well as physical and emotional injury, to Plaintiff.

224. Defendant University of Michigan actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages—including humiliation, embarrassment, loss of dignity, and severe emotional distress—which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

225. Plaintiff and Class Members are entitled to compensatory, consequential, punitive, and nominal damages suffered as a result of the Data Breach.

EIGHTH COUNT
Violation of the Stored Communications Act
Against Only Defendants University of Michigan and Weiss
18 U.S.C. § 2701 *et seq*
(On Behalf of Plaintiff and the Nationwide Class)

226. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

227. The Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, prohibits the intentional access of web-based cloud storage and media accounts, including email or other online databases (including Keffer’s Athletic Trainer System), that contain personal, private, and intimate information.

228. Any person who intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided 18 U.S.C. § 2701(b).

229. Plaintiff’s and Class Members’ electronic information and communications were in electronic storage and fit directly within the protections of the statute. The information, messages, files, and media were accessed by Defendant Weiss without authorization, in part, and

over the course of two years, in connection with his employment with the University of Michigan.

230. Weiss's access without authorization, in part, in connection with his University of Michigan job duties as an athletic coach were intentional and knowingly perpetrated.

231. Defendant Weiss's access to Keffer and to other sources of students stored communications were heightened and supported by his status as an employee of the University of Michigan, working in the capacity of an athletic trainer and coach hired by the University of Michigan, with access to Keffer's Athletic Trainer System.

232. Because Defendant Weiss violated the Stored Communications Act within the scope of his employment as an athletic trainer and Coach at the University of Michigan—which gave him high level security access to Keffer's database of student PHI and PII—the University of Michigan is also liable for the actions of Defendant Weiss to violate the Stored Communications Act.

233. The University of Michigan is vicariously liable for Defendant Weiss's actions because he committed these actions in furtherance of his role as an employee of the University of Michigan. The University of Michigan is liable for completed offenses carried out by Defendant Weiss.

234. Plaintiff and Class Members may assert a claim under § 2707 of the Stored Communications Act, for which there is strict liability.

235. The Stored Communications Act provides that a person aggrieved by a violation of the act may seek appropriate relief including equitable and declaratory relief, actual damages or damages no less than \$1,000, punitive damages, and reasonable attorney's fee[s] and other litigation costs reasonably incurred according to 18 U.S.C. § 2707(b)-(c).

236. Defendant Weiss's access to Plaintiff's and Class Members' private, personal, and

intimate information, messages, files, and media was in violation of 18 U.S.C. § 2701(a). As described above, the University of Michigan is also liable for this access which was, for two years, perpetrated in the scope of his employment by the University of Michigan.

237. Defendant Weiss knew he did not have authority to access Plaintiff's and Class Members' private, personal, and intimate information, messages, files, and media but accessed them nevertheless with intentionality.

238. Under the statute, Plaintiff and Class Members should be granted the greater of (1) the sum of their actual damages suffered as a result of the violations or (2) \$1,000 per violation of the Stored Communications Act.

239. Plaintiff and Class Members are entitled to compensatory, consequential, punitive, and nominal damages suffered as a result of the Data Breach, and attorneys' fees and costs.

NINTH COUNT
Violation of the Computer Fraud and Abuse Act
Against Only Defendants University of Michigan Weiss
18 U.S.C. § 1030, *et seq.*
(On Behalf of Plaintiff and the Nationwide Class)

240. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein

241. Defendant Weiss violated the Computer Fraud and Abuse Act ("CFAA") by unlawfully accessing Plaintiff's private information without authorization.

242. Defendant Weiss did so in the course of his assigned job responsibilities at the University of Michigan where he worked as a trainer and Coach and therefore was provided with heightened access to Keffer's Athletic Trainer System by the University of Michigan.

243. Defendant Weiss's actions constitute a violation of the Act because he "knowingly accessed a computer without authorization" and/or "exceeded authorized access, thereby

obtaining... information.” 18 U.S.C. § 1030(a)(2)(C).

244. Under the CFAA, Defendant Weiss surpassed the scope of his permitted access by entering restricted areas of the digital network and exfiltrating sensitive PHI and PII of students for which he was not authorized to access or download.

245. As described above, Defendant Weiss’s actions were intentional, as he exploited Keffer’s and the University of Michigan’s security failures to prey on students.

246. The University of Michigan is vicariously liable for his actions because he committed these actions in furtherance of his role as an employee of the University. The University of Michigan is liable for completed offenses carried out by Defendant Weiss.

247. Under 18 U.S.C. § 1030(g), Plaintiff and Class Members may recover damages in this civil action from Defendant Weiss and the University of Michigan along with injunctive relief or other equitable relief.

248. Defendants University of Michigan and Weiss actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages—including humiliation, embarrassment, loss of dignity, and severe emotional distress— which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

249. Plaintiff and Class Members are entitled to compensatory, consequential, punitive, and nominal damages suffered as a result of the Data Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, prays for relief as follows:

- A. For an Order certifying this case as a class action and appointing Plaintiff and Plaintiff’s counsel to represent the Class;

- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;
- C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;
- D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
- E. Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;
- F. Ordering Defendant to disseminate individualized notice of the Data Breach to all Class Members;
- G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- I. Pre- and post-judgment interest on any amounts awarded; and
- J. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury of all claims so triable.

Dated: April 8, 2025

Respectfully submitted,

/s/ Gary M. Klinger

Gary M. Klinger

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC

227 W. Monroe Street, Suite 2100

Chicago, IL 60606

Tel: (866) 252-0878

gklinger@milberg.com

James J. Pizzirusso

Amanda V. Boltax*

HAUSFELD LLP

888 16th Street N.W., Suite 300

Washington, D.C. 20006

T: 202.540.7200

jpizzirusso@hausfeld.com

mboltax@hausfeld.com

Steven M. Nathan

Ashley M. Crooks*

HAUSFELD LLP

33 Whitehall Street 14th Floor

New York, New York 10004

T: 646.357.1100

acrooks@hausfeld.com

Counsel for Student Doe

**Application for Pro Hac Vice forthcoming*

EXHIBIT A

From: "U.S. Department of Justice - VNS" <fedemail@vns.usdoj.gov>

Date: March 26, 2025 at 3:26:43 PM CDT

[REDACTED]

**Subject: U.S. Department of Justice - VNS - Investigative Case 288A-DE-3728795
- Court Case 25-CR-20165**

DO NOT REPLY TO THIS EMAIL.



March 26, 2025

[REDACTED]

U.S. Department of Justice

Eastern District of Michigan

Suite 2001

211 W. Fort St.

Detroit, MI 48226-3211

Phone: 1-844-527-5299

Email: USAEO.MCAP@usdoj.gov

Re: United States v. Defendant(s) Matthew Weiss
Case Number 2023R00208 and Court Docket Number 25-CR-20165

Dear [REDACTED]

The enclosed information is provided by the United States Department of Justice

Victim Notification System (VNS). As a victim witness professional, my role is to assist you with information and services during the prosecution of this case. I am contacting you because you were identified by law enforcement as a victim or potential victim during the investigation of the above criminal case.

Should you have questions concerning this case, please contact the Mega Victim Case Assistance Program (MCAP) toll free 1-844-527-5299 (Monday through Friday from 8:30 am to 5:30 pm Eastern), or send an email to USAEO.MCAP@usdoj.gov. Please include your Victim Identification Number (VIN), found in the closing paragraph of this notification, when contacting MCAP via phone or email. If you are having technical difficulties with the Victim Notification System, please contact the VNS Help Desk at the numbers found in the closing of this notification.

Charges have been filed against defendant(s) Matthew Weiss. The lead prosecutor for this case is Timothy Wyse. The main charge is categorized as Other White Collar Crime/Fraud.

If you are receiving this notification, it means that information of yours was found in possession of the defendant.

Pursuant to the Crime Victims' Rights Act, found at Title 18 U.S.C. § 3771, victims have the following rights:

(1) The right to be reasonably protected from the accused; (2) The right to reasonable, accurate, and timely notice of any public court proceeding, or any parole proceeding, involving the crime or of any release or escape of the accused; (3) The right not to be excluded from any such public court proceeding, unless the court, after receiving clear and convincing evidence, determines that testimony by the victim would be materially altered if the victim heard other testimony at that proceeding; (4) The right to be reasonably heard at any public proceeding in the district court involving release, plea, sentencing, or any parole proceeding; (5) The reasonable right to confer with the attorney for the Government in the case; (6) The right to full and timely restitution as provided in law; (7) The right to proceedings free from unreasonable delay; (8) The right to be treated with fairness and with respect for the victim's dignity and privacy; (9) The right to be informed in a timely manner of any plea bargain or deferred prosecution agreement; and (10) The right to be informed of the rights under this section and the services described in section 503(c) of the Victims' Rights and Restitution Act of 1990 (34 U.S.C. § 20141 (c)) and provided contact information for the Office of the Victims' Rights Ombudsman of the Department of Justice.

We will make our best efforts to ensure you are provided the rights to which you are entitled by law. Please understand that these rights apply only to victims of the counts charged in federal court. If you have any questions about what this means for you, please contact our office. Separately, victims of all crimes under federal investigation are entitled to services under the Victims' Rights and Restitution Act (VRRRA), including notification of court events. For further details, please refer to Title 34 U.S.C. § 20141 or the VRRRA link posted at www.notify.usdoj.gov (under the "Related Links"

tab, see "Victim Rights").

It is important to keep in mind that the defendant(s) is/are presumed innocent until proven guilty. Additionally, please be aware that many criminal cases are resolved by a plea agreement between the prosecutor's office and the defendant. You should also know that it is not unusual for a defendant to seek to negotiate a plea agreement shortly before a trial is scheduled to begin. If the court schedules a plea hearing in this case, we will make our best efforts to notify you as soon as practicable.

As mentioned above, you have the right to confer with the attorney for the government. If you would like to speak with the prosecutor to inform the prosecutor of your views regarding potential plea agreements or discuss any other aspect of the case, please contact our office at 1-844-527-5299 and ask to speak to the victim assistance staff, and we will arrange for you to speak with the prosecutor. While our office cannot act as your attorney or provide you with legal advice, you can seek the advice of an attorney with respect to the rights described above or other related legal matters.

If you believe that a Department of Justice employee has not provided you with your rights under the Crime Victims' Rights Act, you may file a complaint with the Department of Justice Victims' Rights Ombudsman (or "Ombuds"). For more information, go to www.justice.gov/usao/office-victims-rights-ombuds. If you have questions about filing a complaint, you may contact the Ombudsman by phone at 1-877-574-9302 or by email at USAEO.VictimOmbudsman@usdoj.gov.

If you have questions about the progress of your case, the rights you are entitled to, or how you can assert your rights during court proceedings, please contact our office at 1-844-527-5299.

Custody of a defendant during a federal criminal case is determined by the Court and is managed by the United States Marshal Service. Custody status of a defendant is subject to change during the course of the criminal proceedings. To receive the timeliest update to your case, please provide and verify your email address, as instructed below.

As of March 24, 2025, Matthew Weiss is not in the custody of the U.S. Marshal Service.

Due to the large number of victims this office receives, you will likely not receive additional correspondence by mail but notice will continue to be available by the other means provided by VNS including email. Through the Victim Notification System (VNS) we will continue to provide you with updated scheduling and event information as the case proceeds through the criminal justice system. You may obtain current information about this case on the VNS website at <https://www.notify.usdoj.gov> or from the VNS Call Center at 1-866-DOJ-4YOU (1-866-365-4968) (TDD/TTY: 1-866-228-4619) (International: 1-502-213-2767). In addition, you may use the Call Center or Internet to update your contact information and/or change your decision about participation in the notification program.

[REDACTED]

[REDACTED]

Remember, VNS is an automated system and cannot answer questions. If you have other questions which involve this matter, please contact this office at the number listed above.

Sincerely,

Alexandra Wyatt
Victim Services Coordinator

If you do not want to receive email notifications from the Victim Notification System (VNS) please log into the VNS Web site at <https://www.notify.usdoj.gov>, select "My Information", remove your email address and click the "update" button. If you remove your email address, you will continue to receive letters from VNS except in those case which have large numbers of victims. To change your email address, select "My Information", provide a new address and click the "update" button.

If you do not want to receive any notifications in your case, select "Stop Receiving Notifications" and follow the instructions on the screen.

If you believe you have received this email in error, please contact the office listed at top of the email message.

Please note, if this is the first notification you have received from VNS you will need to wait 4-8 hours from receipt of this email before you can login to the VNS Internet site (<https://www.notify.usdoj.gov>). In addition, it will also be 4-8 hours before any documents which may have been uploaded to VNS as part of this notification are available under the "Downloads/Links" section on the Web page.

Please call the Victim Notification System (VNS) Help Desk at phone number 1-866-625-1631 for assistance and questions.

Attachments have been referenced with this notification and are available on the VNS Internet site (or will be available within 8 hours). After you log into the website select "Downloads/Links" to view the attachments.

[REDACTED]

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

STUDENT DOE, on behalf of herself and all others similarly situated

(b) County of Residence of First Listed Plaintiff Out-of State-Arkansas
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Gary M. Klinger, Milberg Coleman Bryson Phillips Grossman PLLC
227 W. Monroe Street, Suite 2100, Chicago, IL 60606
Tel: (866) 252-0878

DEFENDANTS

THE UNIVERSITY OF MICHIGAN BOARD OF REGENTS,
KEFFER DEVELOPMENT SERVICES, LLC, and MATTHEW WEISS

County of Residence of First Listed Defendant Washtenaw County, MI
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF
THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

☐ 1 U.S. Government Plaintiff

☐ 3 Federal Question *(U.S. Government Not a Party)*

☐ 2 U.S. Government Defendant

☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

	PTF	DEF		PTF	DEF
Citizen of This State	<input type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business In This State	<input type="checkbox"/> 4	<input checked="" type="checkbox"/> 4
Citizen of Another State	<input checked="" type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business In Another State	<input type="checkbox"/> 5	<input type="checkbox"/> 5
Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
☐ 110 Insurance
☐ 120 Marine
☐ 130 Miller Act
☐ 140 Negotiable Instrument
☐ 150 Recovery of Overpayment & Enforcement of Judgment
☐ 151 Medicare Act
☐ 152 Recovery of Defaulted Student Loans *(Excludes Veterans)*
☐ 153 Recovery of Overpayment of Veteran's Benefits
☐ 160 Stockholders' Suits
☐ 190 Other Contract
☐ 195 Contract Product Liability
☐ 196 Franchise

TORTS
PERSONAL INJURY
☐ 310 Airplane
☐ 315 Airplane Product Liability
☐ 320 Assault, Libel & Slander
☐ 330 Federal Employers' Liability
☐ 340 Marine
☐ 345 Marine Product Liability
☐ 350 Motor Vehicle
☐ 355 Motor Vehicle Product Liability
☒ 360 Other Personal Injury
☐ 362 Personal Injury - Medical Malpractice
PERSONAL INJURY
☐ 365 Personal Injury - Product Liability
☐ 367 Health Care/Pharmaceutical Personal Injury Product Liability
☐ 368 Asbestos Personal Injury Product Liability
PERSONAL PROPERTY
☐ 370 Other Fraud
☐ 371 Truth in Lending
☐ 380 Other Personal Property Damage
☐ 385 Property Damage Product Liability

REAL PROPERTY
☐ 210 Land Condemnation
☐ 220 Foreclosure
☐ 230 Rent Lease & Ejectment
☐ 240 Torts to Land
☐ 245 Tort Product Liability
☐ 290 All Other Real Property

CIVIL RIGHTS
☐ 440 Other Civil Rights
☐ 441 Voting
☐ 442 Employment
☐ 443 Housing/Accommodations
☐ 445 Amer. w/Disabilities - Employment
☐ 446 Amer. w/Disabilities - Other
☐ 448 Education

PRISONER PETITIONS
Habeas Corpus:
☐ 463 Alien Detainee
☐ 510 Motions to Vacate Sentence
☐ 530 General
☐ 535 Death Penalty
Other:
☐ 540 Mandamus & Other
☐ 550 Civil Rights
☐ 555 Prison Condition
☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
☐ 625 Drug Related Seizure of Property 21 USC 881
☐ 690 Other
LABOR
☐ 710 Fair Labor Standards Act
☐ 720 Labor/Management Relations
☐ 740 Railway Labor Act
☐ 751 Family and Medical Leave Act
☐ 790 Other Labor Litigation
☐ 791 Employee Retirement Income Security Act
IMMIGRATION
☐ 462 Naturalization Application
☐ 465 Other Immigration Actions

BANKRUPTCY
☐ 422 Appeal 28 USC 158
☐ 423 Withdrawal 28 USC 157
PROPERTY RIGHTS
☐ 820 Copyrights
☐ 830 Patent
☐ 835 Patent - Abbreviated New Drug Application
☐ 840 Trademark
☐ 880 Defend Trade Secrets Act of 2016
SOCIAL SECURITY
☐ 861 HIA (1395ff)
☐ 862 Black Lung (923)
☐ 863 DIWC/DIWW (405(g))
☐ 864 SSID Title XVI
☐ 865 RSI (405(g))
FEDERAL TAX SUITS
☐ 870 Taxes (U.S. Plaintiff or Defendant)
☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
☐ 375 False Claims Act
☐ 376 Qui Tam (31 USC 3729(a))
☐ 400 State Reapportionment
☐ 410 Antitrust
☐ 430 Banks and Banking
☐ 450 Commerce
☐ 460 Deportation
☐ 470 Racketeer Influenced and Corrupt Organizations
☐ 480 Consumer Credit (15 USC 1681 or 1692)
☐ 485 Telephone Consumer Protection Act
☐ 490 Cable/Sat TV
☐ 850 Securities/Commodities/Exchange
☐ 890 Other Statutory Actions
☐ 891 Agricultural Acts
☐ 893 Environmental Matters
☐ 895 Freedom of Information Act
☐ 896 Arbitration
☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding

☐ 2 Removed from State Court

☐ 3 Remanded from Appellate Court

☐ 4 Reinstated or Reopened

☐ 5 Transferred from Another District *(specify)*

☐ 6 Multidistrict Litigation - Transfer

☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION
Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity):*
28 U.S.C. § 1332(d)
Brief description of cause:
Data Breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND \$
\$5,000,000.00

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY *(See instructions):*
JUDGE Dist. Judge Mark A. Goldsmith
Mag. Judge David R. Grand
DOCKET NUMBER 2:25-cv-10806-MAG-DRG

DATE April 8, 2025
SIGNATURE OF ATTORNEY OF RECORD
/s/ Gary M. Klinger

FOR OFFICE USE ONLY
RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

PURSUANT TO LOCAL RULE 83.11

1. Is this a case that has been previously dismissed?

☐ Yes
☒ No

If yes, give the following information:

Court: _____

Case No.: _____

Judge: _____

2. Other than stated above, are there any pending or previously discontinued or dismissed companion cases in this or any other court, including state court? (Companion cases are matters in which it appears substantially similar evidence will be offered or the same or related parties are present and the cases arise out of the same transaction or occurrence.)

☒ Yes
☐ No

If yes, give the following information:

Court: USDC Eastern District of Michigan

Case No.: 2:25-cv-10855-MAG-DRG; 2:25-cv-10870-MAG-DRG; 2:25-cv-10876-MAG-DRG;
2:25-cv-10946-MAG-DRG; 2:25-cv-10951-MAG-DRG

Judge: Dist. Judge Mark A. Goldsmith/ Mag. Judge David R. Grand

Notes :

**U.S. District Court
Eastern District of Michigan (Detroit)
CIVIL DOCKET FOR CASE #: 2:25-cv-10946-MAG-EAS**

****CASE CLOSED ALL ENTRIES MUST BE MADE IN 25-cv-10806.**** Doe 1 et al v. The Regents Of The University Of Michigan et al
Assigned to: District Judge Mark A. Goldsmith
Referred to: Magistrate Judge Elizabeth A. Stafford
Cause: 28:1331 Fed. Question

Date Filed: 04/02/2025
Date Terminated: 05/23/2025
Jury Demand: Plaintiff
Nature of Suit: 360 P.I.: Other
Jurisdiction: Federal Question

Plaintiff

Jane Doe
I

represented by **Beth M. Rivers**
Pitt McGehee Palmer & Rivers
117 W. Fourth Street
Suite 200
Royal Oak, MI 48067-3804
248-398-9800
Email: brivers@pittlawpc.com
ATTORNEY TO BE NOTICED

Danielle Young Canepa
Pitt McGehee Palmer Bonanni & Rivers PC
117 W. 4th Street
Suite 200
Royal Oak, MI 48067
248-398-9800
Email: dcanepa@pittlawpc.com
ATTORNEY TO BE NOTICED

Jason J. Thompson
Sommers Schwartz, P.C.
One Towne Square
Suite 1700
Southfield, MI 48076
248-355-0300
Fax: 248-436-8453
Email: jthompson@sommerspc.com
ATTORNEY TO BE NOTICED

Kevin Michael Carlson
Pitt McGehee Palmer & Rivers PC
117 West Fourth Street
Suite 200
Royal Oak, MI 48067
248-398-9800
Email: kcarlson@pittlawpc.com
ATTORNEY TO BE NOTICED

Matthew G. Curtis

Sommers Schwartz, P.C.
One Towne Square
17th Floor
Southfield
Southfield, MI 48076
248-746-4038
Fax: 248-936-2124
Email: mcurtis@sommerspc.com
ATTORNEY TO BE NOTICED

Megan Bonanni
Pitt, McGehee,
117 W. Fourth Street
Suite 200
Royal Oak, MI 48067-3804
248-398-9800
Email: mbonanni@pittlawpc.com
ATTORNEY TO BE NOTICED

Richard L. Groffsky
Sommers Schwartz
One Towne Center
Ste 1700
Southfield, MI 48076
248-746-4028
Email: rgroffsky@sommerspc.com
ATTORNEY TO BE NOTICED

Sara Mickovic
Sommers Schwartz, P.C.
1 Towne Square
#1700
Southfield, MI 48076
248-916-2730
Email: smickovic@sommerspc.com
ATTORNEY TO BE NOTICED

Yana A. Hart
Clarkson Law Firm
22525 Pacific Coast Highway
Malibu, CA 90265
213-788-4050
Email: yhart@clarksonlawfirm.com
ATTORNEY TO BE NOTICED

Lisa M. Esser
Sommers Schwartz, P.C.
One Towne Square
Ste 1700
Southfield, MI 48076
248-355-0300
Email: lesser@sommerspc.com
ATTORNEY TO BE NOTICED

Plaintiff**Jane Doe**

2

represented by **Beth M. Rivers**

(See above for address)

*ATTORNEY TO BE NOTICED***Danielle Young Canepa**

(See above for address)

*ATTORNEY TO BE NOTICED***Jason J. Thompson**

(See above for address)

*ATTORNEY TO BE NOTICED***Kevin Michael Carlson**

(See above for address)

*ATTORNEY TO BE NOTICED***Matthew G. Curtis**

(See above for address)

*ATTORNEY TO BE NOTICED***Megan Bonanni**

(See above for address)

*ATTORNEY TO BE NOTICED***Richard L. Groffsky**

(See above for address)

*ATTORNEY TO BE NOTICED***Sara Mickovic**

(See above for address)

*ATTORNEY TO BE NOTICED***Yana A. Hart**

(See above for address)

*ATTORNEY TO BE NOTICED***Lisa M. Esser**

(See above for address)

*ATTORNEY TO BE NOTICED***Plaintiff****Jane Doe**

3

represented by **Beth M. Rivers**

(See above for address)

*ATTORNEY TO BE NOTICED***Danielle Young Canepa**

(See above for address)

*ATTORNEY TO BE NOTICED***Jason J. Thompson**

(See above for address)

ATTORNEY TO BE NOTICED

Kevin Michael Carlson
(See above for address)
ATTORNEY TO BE NOTICED

Matthew G. Curtis
(See above for address)
ATTORNEY TO BE NOTICED

Megan Bonanni
(See above for address)
ATTORNEY TO BE NOTICED

Richard L. Groffsky
(See above for address)
ATTORNEY TO BE NOTICED

Robert J. Lantzy
Buckfire & Buckfire
29000 Inkster Road
Ste. 150
Southfield, MI 48034
248-569-4646
Email: robert@buckfirelaw.com
ATTORNEY TO BE NOTICED

Sara Mickovic
(See above for address)
ATTORNEY TO BE NOTICED

Yana A. Hart
(See above for address)
ATTORNEY TO BE NOTICED

Lisa M. Esser
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Jane Doe

4

represented by **Beth M. Rivers**
(See above for address)
ATTORNEY TO BE NOTICED

Danielle Young Canepa
(See above for address)
ATTORNEY TO BE NOTICED

Jason J. Thompson
(See above for address)
ATTORNEY TO BE NOTICED

Kevin Michael Carlson
(See above for address)
ATTORNEY TO BE NOTICED

Matthew G. Curtis
(See above for address)
ATTORNEY TO BE NOTICED

Megan Bonanni
(See above for address)
ATTORNEY TO BE NOTICED

Richard L. Groffsky
(See above for address)
ATTORNEY TO BE NOTICED

Sara Mickovic
(See above for address)
ATTORNEY TO BE NOTICED

Yana A. Hart
(See above for address)
ATTORNEY TO BE NOTICED

Lisa M. Esser
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Jane Doe
5

represented by **Beth M. Rivers**
(See above for address)
ATTORNEY TO BE NOTICED

Danielle Young Canepa
(See above for address)
ATTORNEY TO BE NOTICED

Jason J. Thompson
(See above for address)
ATTORNEY TO BE NOTICED

Kevin Michael Carlson
(See above for address)
ATTORNEY TO BE NOTICED

Matthew G. Curtis
(See above for address)
ATTORNEY TO BE NOTICED

Megan Bonanni
(See above for address)
ATTORNEY TO BE NOTICED

Richard L. Groffsky
(See above for address)
ATTORNEY TO BE NOTICED

Sara Mickovic

(See above for address)

ATTORNEY TO BE NOTICED

Yana A. Hart

(See above for address)

ATTORNEY TO BE NOTICED

Lisa M. Esser

(See above for address)

ATTORNEY TO BE NOTICED

Plaintiff

Jane Doe

6

represented by **Beth M. Rivers**

(See above for address)

ATTORNEY TO BE NOTICED

Danielle Young Canepa

(See above for address)

ATTORNEY TO BE NOTICED

Jason J. Thompson

(See above for address)

ATTORNEY TO BE NOTICED

Kevin Michael Carlson

(See above for address)

ATTORNEY TO BE NOTICED

Matthew G. Curtis

(See above for address)

ATTORNEY TO BE NOTICED

Megan Bonanni

(See above for address)

ATTORNEY TO BE NOTICED

Richard L. Groffsky

(See above for address)

ATTORNEY TO BE NOTICED

Sara Mickovic

(See above for address)

ATTORNEY TO BE NOTICED

Yana A. Hart

(See above for address)

ATTORNEY TO BE NOTICED

Lisa M. Esser

(See above for address)

ATTORNEY TO BE NOTICED

Plaintiff

Jane Doe

7

represented by **Beth M. Rivers**

(See above for address)

*ATTORNEY TO BE NOTICED***Danielle Young Canepa**

(See above for address)

*ATTORNEY TO BE NOTICED***Jason J. Thompson**

(See above for address)

*ATTORNEY TO BE NOTICED***Kevin Michael Carlson**

(See above for address)

*ATTORNEY TO BE NOTICED***Matthew G. Curtis**

(See above for address)

*ATTORNEY TO BE NOTICED***Megan Bonanni**

(See above for address)

*ATTORNEY TO BE NOTICED***Richard L. Groffsky**

(See above for address)

*ATTORNEY TO BE NOTICED***Sara Mickovic**

(See above for address)

*ATTORNEY TO BE NOTICED***Yana A. Hart**

(See above for address)

*ATTORNEY TO BE NOTICED***Lisa M. Esser**

(See above for address)

*ATTORNEY TO BE NOTICED***Plaintiff****Jane Doe**

8

represented by **Beth M. Rivers**

(See above for address)

*ATTORNEY TO BE NOTICED***Danielle Young Canepa**

(See above for address)

*ATTORNEY TO BE NOTICED***Jason J. Thompson**

(See above for address)

*ATTORNEY TO BE NOTICED***Kevin Michael Carlson**

(See above for address)
ATTORNEY TO BE NOTICED

Matthew G. Curtis
(See above for address)
ATTORNEY TO BE NOTICED

Megan Bonanni
(See above for address)
ATTORNEY TO BE NOTICED

Richard L. Groffsky
(See above for address)
ATTORNEY TO BE NOTICED

Robert J. Lantzy
(See above for address)
ATTORNEY TO BE NOTICED

Sara Mickovic
(See above for address)
ATTORNEY TO BE NOTICED

Yana A. Hart
(See above for address)
ATTORNEY TO BE NOTICED

Lisa M. Esser
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Jane Doe
9

represented by **Beth M. Rivers**
(See above for address)
ATTORNEY TO BE NOTICED

Danielle Young Canepa
(See above for address)
ATTORNEY TO BE NOTICED

Jason J. Thompson
(See above for address)
ATTORNEY TO BE NOTICED

Kevin Michael Carlson
(See above for address)
ATTORNEY TO BE NOTICED

Matthew G. Curtis
(See above for address)
ATTORNEY TO BE NOTICED

Megan Bonanni
(See above for address)

ATTORNEY TO BE NOTICED

Richard L. Groffsky

(See above for address)

ATTORNEY TO BE NOTICED

Robert J. Lantzy

(See above for address)

ATTORNEY TO BE NOTICED

Sara Mickovic

(See above for address)

ATTORNEY TO BE NOTICED

Yana A. Hart

(See above for address)

ATTORNEY TO BE NOTICED

Lisa M. Esser

(See above for address)

ATTORNEY TO BE NOTICED

Plaintiff

Jane Doe

10

represented by **Beth M. Rivers**

(See above for address)

ATTORNEY TO BE NOTICED

Danielle Young Canepa

(See above for address)

ATTORNEY TO BE NOTICED

Jason J. Thompson

(See above for address)

ATTORNEY TO BE NOTICED

Kevin Michael Carlson

(See above for address)

ATTORNEY TO BE NOTICED

Matthew G. Curtis

(See above for address)

ATTORNEY TO BE NOTICED

Megan Bonanni

(See above for address)

ATTORNEY TO BE NOTICED

Richard L. Groffsky

(See above for address)

ATTORNEY TO BE NOTICED

Sara Mickovic

(See above for address)

ATTORNEY TO BE NOTICED

Yana A. Hart

(See above for address)

ATTORNEY TO BE NOTICED

Lisa M. Esser

(See above for address)

ATTORNEY TO BE NOTICED

Plaintiff

Jane Doe

II

represented by **Beth M. Rivers**

(See above for address)

ATTORNEY TO BE NOTICED

Danielle Young Canepa

(See above for address)

ATTORNEY TO BE NOTICED

Jason J. Thompson

(See above for address)

ATTORNEY TO BE NOTICED

Kevin Michael Carlson

(See above for address)

ATTORNEY TO BE NOTICED

Matthew G. Curtis

(See above for address)

ATTORNEY TO BE NOTICED

Megan Bonanni

(See above for address)

ATTORNEY TO BE NOTICED

Richard L. Groffsky

(See above for address)

ATTORNEY TO BE NOTICED

Sara Mickovic

(See above for address)

ATTORNEY TO BE NOTICED

Yana A. Hart

(See above for address)

ATTORNEY TO BE NOTICED

Lisa M. Esser

(See above for address)

ATTORNEY TO BE NOTICED

V.

Defendant

**The Regents Of The University Of
Michigan**

represented by **Daniel B. Tukel**
Butzel Long
201 West Big Beaver Road
Suite 1200
Troy, MI 48084
313-225-7047
Email: tukel@butzel.com
ATTORNEY TO BE NOTICED

Sheldon H. Klein
Butzel
201 West Big Beaver Road
Suite 1200
Troy, MI 48084
248-258-1414
Fax: 248-258-1439
Email: klein@butzel.com
ATTORNEY TO BE NOTICED

Defendant

University of Michigan

represented by **Daniel B. Tukel**
(See above for address)
ATTORNEY TO BE NOTICED

Sheldon H. Klein
(See above for address)
ATTORNEY TO BE NOTICED

Defendant

Keffer Development Services, LLC

represented by **Carl Andrew Fejko**
Dillon McCandless King Coulter Graham
Civil Practice
128 West Cunningham St.
Butler, PA 16001
724-822-2148
Email: cfejko@dmkcg.com
ATTORNEY TO BE NOTICED

Jordan P. Shuber
Dillon McCandless King Coulter &
Graham, LLP
128 West Cunningham Street
Butler, PA 16001
724-283-2200
Fax: 724-283-2298
Email: jshuber@dmkcg.com
ATTORNEY TO BE NOTICED

Thomas W. King , III
Dillon McCandless King Coulter & Graham
LLP
128 West Cunningham Street
Buter, PA 16001
724-283-2200

Email: tking@dmkcg.com

ATTORNEY TO BE NOTICED

Defendant**Matthew Weiss**

Date Filed	#	Docket Text
04/02/2025	<u>1</u>	COMPLAINT <i>CLASS ACTION</i> filed by All Plaintiffs against All Defendants with Jury Demand. Plaintiff requests summons issued . Receipt No: AMIEDC-10182341 - Fee: \$ 405. County of 1st Plaintiff: Out of State - County Where Action Arose: Washtenaw - County of 1st Defendant: Washtenaw. [Previously dismissed case: No] (Esser, Lisa) (Entered: 04/02/2025)
04/03/2025	<u>2</u>	SUMMONS Issued for *Keffer Development Services, LLC* (LHam) (Entered: 04/03/2025)
04/03/2025	<u>3</u>	SUMMONS Issued for *The Regents Of The University Of Michigan* (LHam) (Entered: 04/03/2025)
04/03/2025	<u>4</u>	SUMMONS Issued for *University of Michigan* (LHam) (Entered: 04/03/2025)
04/03/2025	<u>5</u>	SUMMONS Issued for *Matthew Weiss* (LHam) (Entered: 04/03/2025)
04/03/2025		A United States Magistrate Judge of this Court is available to conduct all proceedings in this civil action in accordance with 28 U.S.C. 636c and FRCP 73. The Notice, Consent, and Reference of a Civil Action to a Magistrate Judge form is available for download at http://www.mied.uscourts.gov (LHam) (Entered: 04/03/2025)
04/03/2025	<u>6</u>	NOTICE of Appearance by Matthew G. Curtis on behalf of All Plaintiffs. (Curtis, Matthew) (Entered: 04/03/2025)
04/03/2025	<u>7</u>	NOTICE of Appearance by Megan Bonanni on behalf of All Plaintiffs. (Bonanni, Megan) (Entered: 04/03/2025)
04/03/2025	<u>8</u>	NOTICE of Appearance by Beth M. Rivers on behalf of All Plaintiffs. (Rivers, Beth) (Entered: 04/03/2025)
04/03/2025	<u>9</u>	ATTORNEY APPEARANCE: Danielle Young Canepa appearing on behalf of All Plaintiffs (Young Canepa, Danielle) (Entered: 04/03/2025)
04/03/2025	<u>10</u>	ATTORNEY APPEARANCE: Kevin Michael Carlson appearing on behalf of All Plaintiffs (Carlson, Kevin) (Entered: 04/03/2025)
04/04/2025	<u>11</u>	[INCORRECTLY REASSIGNED DISTRICT JUDGE INSTEAD OF MAGISTRATE JUDGE] ORDER OF RECUSAL AND REASSIGNING CASE from District Judge Jonathan J.C. Grey to District Judge Nancy G. Edmunds. (NAhm) Modified on 4/4/2025 (NAhm). (Entered: 04/04/2025)
04/04/2025	<u>12</u>	NOTICE of Correction re <u>11</u> Order of Reassignment/Disqualification. (NAhm) (Entered: 04/04/2025)
04/04/2025	<u>13</u>	ORDER OF RECUSAL AND REASSIGNING CASE from Magistrate Judge Anthony P. Patti to Magistrate Judge Curtis Ivy, Jr. (NAhm) (Entered: 04/04/2025)
04/08/2025	<u>14</u>	ORDER REASSIGNING CASE from District Judge Jonathan J.C. Grey and Magistrate Judge Curtis Ivy, Jr to District Judge Mark A. Goldsmith and Magistrate Judge David R. Grand. (NAhm) (Entered: 04/08/2025)

04/08/2025	15	NOTICE of Appearance by Daniel B. Tukul on behalf of The Regents Of The University Of Michigan, University of Michigan. (Tukul, Daniel) (Entered: 04/08/2025)
04/08/2025	16	STIPULATED ORDER EXTENDING TIME TO RESPOND TO COMPLAINT UNTIL JUNE 5, 2025 - Signed by District Judge Mark A. Goldsmith. (CCie) (Entered: 04/08/2025)
04/09/2025	17	NOTICE of Appearance by Jason J. Thompson on behalf of All Plaintiffs. (Thompson, Jason) (Entered: 04/09/2025)
04/10/2025	18	ORDER OF RECUSAL AND REASSIGNING CASE from Magistrate Judge David R. Grand to Magistrate Judge Elizabeth A. Stafford. (NAhm) (Entered: 04/10/2025)
04/15/2025	19	NOTICE of Appearance by Sheldon H. Klein on behalf of The Regents Of The University Of Michigan, University of Michigan. (Klein, Sheldon) (Entered: 04/15/2025)
04/15/2025	20	STIPULATED ORDER EXTENDING TIME TO RESPOND TO COMPLAINT - Signed by District Judge Mark A. Goldsmith. (CCie) (Entered: 04/15/2025)
04/15/2025	21	NOTICE by Jane Doe from 10806 (Attachments: # 1 Exhibit) (Stinar, Parker) Modified on 4/16/2025 (LHam). [NOTICE OF MOTION TO CONSOLIDATE WITH CASE 25-10806 AND NOTICE TO APPOINT LEAD COUNSEL] (Entered: 04/15/2025)
04/16/2025	22	NOTICE by The Regents Of The University Of Michigan, University of Michigan <i>of filing Motion to Consolidate in case 25-cv-10806</i> (Tukul, Daniel) (Entered: 04/16/2025)
04/17/2025	23	MOTION for Status Conference by All Plaintiffs. (Attachments: # 1 Exhibit 1 - Keffer Attorney Letter, # 2 Exhibit 2 - Illinois Complaint, # 3 Exhibit 3 - Jason Thompson Declaration) (Thompson, Jason) (Entered: 04/17/2025)
04/21/2025	24	AMENDED COMPLAINT with Jury Demand filed by All Plaintiffs against All Defendants. NO NEW PARTIES ADDED. (Attachments: # 1 Exhibit Exhibit A, # 2 Exhibit Exhibit B) (Esser, Lisa) (Entered: 04/21/2025)
04/22/2025	25	WAIVER OF SERVICE Returned Executed. Keffer Development Services, LLC waiver sent on 4/21/2025, answer due 6/20/2025. (Esser, Lisa) (Entered: 04/22/2025)
04/22/2025	26	ORDER Regarding Status Conference. Signed by District Judge Mark A. Goldsmith. (HRya) (Entered: 04/22/2025)
04/22/2025	27	NOTICE TO APPEAR REMOTELY: Status Conference set for 5/14/2025 at 9:00 AM before District Judge Mark A. Goldsmith. (HRya) (Entered: 04/22/2025)
04/24/2025	28	ATTORNEY APPEARANCE: Richard L. Groffsky appearing on behalf of All Plaintiffs (Groffsky, Richard) (Entered: 04/24/2025)
04/24/2025	29	NOTICE by Jane Doe from 10806 <i>Majority Plaintiffs' Amended Motion</i> (Stinar, Parker) (Entered: 04/24/2025)
05/09/2025	30	MOTION Plaintiff Counsels' Motion for Appointment of Interim Class Counsel by All Plaintiffs. (Attachments: # 1 Index of Exhibits, # 2 Exhibit A - Sommers Schwartz Attorney Bios, # 3 Exhibit B - Pitt McGehee Attorney Bios, # 4 Exhibit C - Clarkson Firm Attorney Bios, # 5 Exhibit D - Marko Firm Attorney Bio, # 6 Exhibit E - Weiss Indictment, # 7 Exhibit F - Illinois Complaint, # 8 Exhibit G - Ohio Complaint, # 9 Exhibit H - Massachusetts Complaint, # 10 Exhibit I - North Carolina Complaint, # 11 Exhibit J - California Complaint, # 12 Exhibit K - Michigan Court of Claims Complaint, # 13 Exhibit L - Midland Dam Case Order re Liaison Counsel) (Thompson, Jason) (Entered: 05/09/2025)

05/12/2025	31	NOTICE by All Plaintiffs re 30 MOTION Plaintiff Counsels' Motion for Appointment of Interim Class Counsel <i>Notice of Filing Corrected Page 1</i> (Attachments: # 1 Exhibit Corrected Page 1) (Thompson, Jason) (Entered: 05/12/2025)
05/12/2025	32	NOTICE of Appearance by Sara Mickovic on behalf of All Plaintiffs. (Mickovic, Sara) (Entered: 05/12/2025)
05/12/2025	33	NOTICE of Joinder/Concurrence in 30 MOTION Plaintiff Counsels' Motion for Appointment of Interim Class Counsel filed by Jane Doe by Jane Doe, Jane Doe, Jane Doe (Lantzy, Robert) (Entered: 05/12/2025)
05/14/2025	34	NOTICE of Appearance by Thomas W. King, III on behalf of Keffer Development Services, LLC. (King, Thomas) (Entered: 05/14/2025)
05/14/2025		Minute Entry for remote proceedings before District Judge Mark A. Goldsmith: Status Conference held on 5/14/2025. (Court Reporter: None Present, Not on the Record) (JHea) (Entered: 05/14/2025)
05/14/2025	35	NOTICE of Appearance by Carl Andrew Fejko on behalf of Keffer Development Services, LLC. (Fejko, Carl) (Entered: 05/14/2025)
05/15/2025	36	NOTICE of Appearance by Jordan P. Shuber on behalf of Keffer Development Services, LLC. (Shuber, Jordan) (Entered: 05/15/2025)
05/16/2025	37	NOTICE by Jane Doe, Jane Doe, Jane Doe, Jane Doe, Jane Doe, Jane Doe, Jane Doe, Jane Doe, Jane Doe, Jane Doe re: <i>Supplemental Memorandum in Support of Plaintiff Counsels Motion for Appointment of Interim Class Counsel</i> (Attachments: # 1 Exhibit A) (Hart, Yana) (Entered: 05/16/2025)
05/23/2025	38	ORDER FOR CONSOLIDATION AND RELATED MATTERS. Signed by District Judge Mark A. Goldsmith. (JHea) (Entered: 05/23/2025)
05/23/2025	39	Notice to Parties Regarding Consolidated Case: Order of consolidation entered on *5/23/2025*. Designated lead case number is *25-10806*. (JHea) (Entered: 05/23/2025)

PACER Service Center			
Transaction Receipt			
06/05/2025 16:34:18			
PACER Login:	ThomaKingtking	Client Code:	
Description:	Docket Report	Search Criteria:	2:25-cv-10946-MAG-EAS
Billable Pages:	17	Cost:	1.70

NITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

JANE DOE 1, JANE DOE 2,
JANE DOE 3, JANE DOE 4,
JANE DOE 5, JANE DOE 6,
JANE DOE 7, JANE DOE 8,
JANE DOE 9, JANE DOE 10,
and JANE DOE 11,
on behalf of themselves and
others similarly situated,

Plaintiffs,

-vs-

Case No.
Hon.

THE REGENTS OF THE UNIVERSITY OF
MICHIGAN; the UNIVERSITY OF MICHIGAN;
KEFFER DEVELOPMENT SERVICES, LLC,
and MATTHEW WEISS

Defendants.

SOMMERS SCHWARTZ, P.C.
Lisa M. Esser (P70628)
Richard L. Groffsky (P32992)
Jason J. Thompson (P47184)
Matthew G. Curtis (P37999)
Attorney for Plaintiffs
One Towne Square, Suite 1700
Southfield, Michigan, 48076
(248) 355-0300
LEsser@sommerspc.com
RGroffsky@sommerspc.com
JThompson@sommerspc.com
MCurtis@sommerspc.com

PITT MCGEHEE PALMER BONANNI
& RIVERS
Megan A. Bonanni (P52079)
Kevin M. Carlson (P67704)
Beth M. Rivers (P33614)
Danielle Y. Canepa (P82237)

Attorneys for Plaintiffs
117 W. Fourth Street, Suite 200
Royal Oak, MI 48067
(248) 398-9800
mbonnani@pittlawpc.com
kcarlson@pittlawpc.com
brivers@pittlawpc.com
dcanepa@pittlawpc.com

There are pending civil actions arising out of similar transactions or occurrences alleged in this Complaint. Those cases have been filed in this Court for different Plaintiffs under Case Numbers 2:25-cv-10870, 2:25-cv-10855, 2:25-cv-10806 and 2:25-cv-10876.

PLAINTIFFS' CLASS ACTION COMPLAINT

Plaintiffs, JANE DOE 1, JANE DOE 2, JANE DOE 3, JANE DOE 4, JANE DOE 5, JANE DOE 6, JANE DOE 7, JANE DOE 8, JANE DOE 9, JANE DOE 10 and JANE DOE 11 ("Plaintiffs"), through their attorneys, Sommers Schwartz, P.C., and Pitt McGehee Palmer Bonanni & Rivers, P.C., for their Complaint against MATTHEW WEISS, the REGENTS OF THE UNIVERSITY OF MICHIGAN, the UNIVERSITY OF MICHIGAN, and KEFFER DEVELOPMENT SERVICES, LLC, state as follows:

INTRODUCTION

Students and alumni connected to the University of Michigan from 2015 to 2023—many of them student-athletes—have been subjected to a deeply troubling and unlawful breach of privacy, stemming from the actions of former University of Michigan football co-offensive coordinator and quarterback coach Matthew Weiss, whose violations of their privacy were facilitated by yet another recent incident of institutional negligence. This class action lawsuit, filed against Matthew Weiss, the Regents of the University of Michigan, the University itself, and Keffer Development Services, LLC, seeks justice for the unauthorized access and misuse of personal information—an abuse so severe that student-athletes are now receiving formal

notification from the U.S. Department of Justice that their private information has been exposed, including Plaintiffs Jane Doe 10 and Jane Doe 11. This action is brought to hold the Defendants accountable for yet another instance in a developing pattern of their failure to protect those in their care, particularly student athletes, from foreseeable harm.

PARTIES

1. Plaintiff Jane Doe 1 was a student athlete at the University of Michigan between 2017-2020 and was a member of the University of Michigan Women's Gymnastics Team.

2. Plaintiff Jane Doe 1 is domiciled in Harris County, Texas, in the City of Houston.

3. Plaintiff Jane Doe 2 is a student at the University of Michigan and was a student athlete between 2023-2024 and was a member of the Women's Soccer Team.

4. Plaintiff Jane Doe 2 is domiciled in Washtenaw County, Michigan, in the City of Ann Arbor.

5. Plaintiff Jane Doe 3 was a student athlete at the University of Michigan, Dearborn between 2015-2016 and was a member of the University of Michigan, Dearborn Women's Cheerleading Team.

6. Plaintiff Jane Doe 3 is domiciled in Oakland County, Michigan, in the City of Birmingham.

7. Plaintiff Jane Doe 4 was a student athlete at the University of Michigan between 2014-2018, and was a member of the Women's Soccer Team.

8. Plaintiff Jane Doe 4 is domiciled in Oakland County, Michigan, in the City of Rochester.

9. Plaintiff Jane Doe 5 was a student athlete at the University of Michigan between 2014-2018, and was a member of the Women's Soccer Team.

10. Plaintiff Jane Doe 5 is domiciled in Oakland County, Michigan, in the City of West Bloomfield.

11. Plaintiff Jane Doe 6 was a student athlete at the University of Michigan between 2014-2018, and was a member of the Women's Soccer Team.

12. Plaintiff Jane Doe 6 is domiciled in Fulton County, Georgia, in the City of Atlanta.

13. Plaintiff Jane Doe 7 was a student athlete at the University of Michigan between 2014-2018, and was a member of the Women's Soccer Team.

14. Plaintiff Jane Doe 7 is domiciled in Wayne County, Michigan, in the City of Plymouth.

15. Plaintiff Jane Doe 8 was a student athlete at the University of Michigan between 2014-2015, and was a member of the Women's Soccer Team.

16. Plaintiff Jane Doe 8 is domiciled in Orleans Parish, Louisiana, City of New Orleans.

17. Plaintiff Jane Doe 9 was a student athlete at the University of Michigan between 2014-2016, and was a member of the Women's Soccer Team.

18. Plaintiff Jane Doe 9 is domiciled in Missouri, City of St. Louis.

19. Plaintiff Jane Doe 10 was a student athlete at the University of Michigan between 2016-2019 and was a member of the University of Michigan Women's Gymnastics Team.

20. Plaintiff Jane Doe 10 is domiciled in Illinois, City of Chicago.

21. Plaintiff Jane Doe 11 was a student athlete at the University of Maryland and Loyola University Chicago, playing on the respective Volleyball Teams from 2017 to 2021.

22. Plaintiff Jane Doe 11 is domiciled in Illinois, City of Chicago.

23. The Regents of the University of Michigan (“the Regents”) is a corporate entity, with the right to be sued, and is responsible for governing the University of Michigan, pursuant to Mich. Comp. Laws § 390.3 and § 390.4.

24. The University of Michigan (“the University”) is a public university organized and existing under the laws of the State of Michigan.

25. The University has received, and continues to receive, funding from the State of Michigan, making it, among other reasons, subject to the laws of the State of Michigan.

26. Keffer Development Services, LLC (“Keffer”) is a Pennsylvania limited liability company that has continuously and systemically conducted business in Michigan by directly providing services to residents and entities within the State of Michigan, thereby availing itself of protections of the law of the State of Michigan.

27. Any wrongful conduct and legal violations committed by Defendant Keffer that are subsequently outlined in this Complaint occurred specifically with respect to the Plaintiffs that resided in Michigan during the time of the incident alleged in this Complaint.

28. Matthew Weiss (“Weiss”) is an individual residing in the State of Michigan.

JURISDICTION

29. Jurisdiction is proper in this Court under 28 U.S.C. §§ 1331 and 1367 as this matter involves a claim under the Stored Communications Act, 18 U.S.C. § 2701(a) *et seq.*; the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; Title IX, 20 U.S.C. § 1681(A) *et seq.*; 42 U.S.C. § 1983; the Fourth Amendment of the U.S. Constitution; and the Fourteenth Amendment of the U.S. Constitution, and this Court has supplemental jurisdiction of all additional causes of action alleged in this Complaint pursuant to 28 U.S.C. §1367(a); and subject matter jurisdiction pursuant to 28 U.S.C. §1332(d) under the Class Action Fairness Act (“CAFA”) as a class action

lawsuit in which the amount in controversy exceeds \$50,000,000.00, there are more than one-hundred putative class members, and the majority of the putative class members are citizens of a state different than the state of which Defendants are citizens.

30. Venue is appropriate in this district under U.S.C. §1391 since a substantial part of the events giving rise to these claims occurred within, and Defendants conduct or have conducted their businesses in the Eastern District of Michigan.

31. Plaintiffs' injuries are redressable by monetary compensation, and all alleged injuries of Plaintiffs and class members can be traced to Defendants' conduct.

COMMON ALLEGATIONS

32. At all relevant times, Weiss was employed by the University.

33. Upon information and belief, Weiss's actions alleged in this Complaint happened during his employment at the University.

34. The Regents had a responsibility and duty to oversee the University's operations, policies and procedures, and care for and protect the University's students.

35. Keffer had a responsibility and duty to protect the private data of student athletes stored within their database and to have mechanisms in place to prevent such a gross invasion of privacy as what occurred in this case.

36. The risk of identity theft and breaches of security to access users' private, personal, and confidential information is foreseeable within the Defendants' information technology systems, and Defendants are well aware of the foreseeable risks of breaches, such as those alleged in this case, that are likely to occur if their practices in detecting, preventing, and mitigating such breaches are substandard.

37. The Regents and University breached their duty of care when University personnel failed to supervise and monitor Weiss adequately, resulting in the unlawful invasion of privacy of Plaintiffs and over a thousand others.

38. Keffer breached its duty of care when it failed to have adequate measures in place to prevent the hacking by Weiss, resulting in the unlawful invasion of privacy of Plaintiff and over a thousand others.

39. Plaintiffs and putative class members are current and former student-athletes at the University of Michigan and other affected institutions in the United States that were specifically targeted by Weiss and harmed by the violation of their privacy.

40. The Regents are responsible for overseeing the University's operations, finances, budget approvals, policies, construction projects, etc.

41. The Regents failed in this duty by failing to consider, implement, enforce, or follow a policy in which proper oversight and supervision of University personnel, including Weiss, could have ensured that breaches of Plaintiffs' privacy would not have occurred.

42. The Regents failed in this duty by failing to take any action to prevent the harm caused to Plaintiffs and other student-athletes as alleged in this Complaint.

43. The Regents failed in their duty to establish University policies that would include monitoring of personnel, such as Weiss, so the privacy of students, such as Plaintiffs and other student-athletes, would be protected.

44. The Regents and the University were required to ensure that student-athletes, such as Plaintiffs, were not exposed to professionals who would invade their privacy.

45. The Regents and the University were reckless in failing to ensure that media and other private, personal and sensitive information, including but not limited to those of Plaintiffs, was securely protected, as the Regents and the University were entrusted to do so.

46. The Regents, University and Keffer (collectively “The Non-Individual Defendants”) had, and continue to have, a duty to protect Plaintiffs and to take appropriate security measures to protect private, personal, and intimate information and images.

47. This duty was breached by the Non-Individual Defendants when there was a failure to consider or implement adequate security measures to protect these private, personal, and intimate information and images of Plaintiffs and those similarly situated.

48. The Regents had the responsibility to financially oversee the University and all three University of Michigan campuses but failed to ensure this duty was properly exercised when they failed to allocate necessary resources to prevent security breaches and instead prioritized avoiding costs associated with implementing necessary security measures.

49. The University, like the Regents, failed to uphold these responsibilities and engaged in similar breaches of duty despite having all the same duties.

50. Keffer, like the University and Regents, failed to uphold these responsibilities and engaged in similar breaches of duty despite having all the same duties.

51. Plaintiffs, and putative class members, are current and former student-athletes at the University of Michigan and other affected institutions that were specifically targeted by Weiss and harmed by the violation of their privacy by Defendants.

52. Plaintiffs, and those similarly situated, entrusted the Non-Individual Defendants to protect their private, intimate, and personal images and information.

53. The University breached its duty when it recklessly allowed Weiss to access Plaintiffs', and other student-athletes, private information and images and thus invading their privacy.

54. The Regents also breached their general supervision privileges over the University's expenditures after they failed to ensure that the University's millions of public dollars were allocated to protect the privacy of students, including student-athletes', private images and information.

55. The University employed and had authority over Weiss.

56. The University assigned and directed job responsibilities to Weiss.

57. These job responsibilities enabled Weiss to access private, personal, and intimate images and information of Plaintiffs and others similarly situated, all of which were entrusted to the University to be safeguarded.

58. While the University gave Weiss the means to invade the privacy of Plaintiffs and others similarly situated, the University failed to supervise or monitor his actions.

59. The University breached the trust and confidence of Plaintiffs and other student-athletes by granting Weiss the ability and resources to allow him to track, invade, and surveil Plaintiffs and others by invading their personal lives and obtaining images and personal information about them.

60. With no University supervision, Weiss, during his employment with the University, invaded Plaintiffs' privacy and the privacy of other similarly situated student athletes.

61. The Regents, the University, and Weiss all engaged in misconduct, recklessness, and misconduct which also implicated Keffer.

62. Keffer's negligence and reckless disregard contributed to Weiss' privacy violations against Plaintiffs and other student athletes.

63. Keffer agreed to safely maintain and store information, images, expressions, and videos of Plaintiffs and their peers in a secure manner, free from access from unauthorized employees of the University such as Weiss or other unauthorized third parties.

64. Keffer knew that information stored for and by Plaintiffs and others was personal, private, and intimate.

65. Keffer had an express obligation to safeguard and protect the personal, private, and intimate images and information entrusted to Keffer by Plaintiffs and others similar to them.

66. Keffer breached these obligations when they failed to consider, enact, or implement adequate policies, procedures, or security measures to safeguard and protect the personal, private, and intimate images and information entrusted to Keffer by Plaintiffs and others similar to them.

67. As a direct result of Keffer's security failures, Weiss accessed the personal, private, and intimate images and information entrusted to Keffer by Plaintiffs and others similar to them.

68. Keffer collects and stores information including private information about students and student athletes around this nation.

69. The University and the Regents permitted Keffer to collect and store private, personal, and intimate information about students and student athletes.

70. Plaintiffs and others similar to them entrusted that the Regents, the University and Keffer would safeguard their private images and information and ensure the confidentiality of their data.

71. The Regents and the University failed to take reasonable action to ensure that Keffer retained the privacy of the sensitive information of Plaintiffs and others like them.

72. The Regents' negligence in this respect harmed Plaintiffs.

73. The University's negligence in this respect also harmed Plaintiffs.

74. Keffer failed to take appropriate and reasonable action to ensure that it retained the privacy of the images and information of Plaintiffs and others like them entrusted to them.

75. Keffer did not take necessary and reasonable precautions to protect against the access by Weiss of the private information and images of Plaintiffs and those similarly situated.

76. Due to the negligent and reckless conduct of the Non-Individual Defendants, Weiss was able to, and did, unlawfully obtain and misuse private and confidential information belonging to Plaintiffs and other student-athletes like Plaintiffs.

77. Upon information and believe, Weiss unlawfully gained access to the social media, email, cloud storage, and other digital accounts of more than 3,300 people including but not limited to Plaintiffs and other University student athletes that were active between 2015 and 2023, as was detailed in the federal criminal indictment against him, and which is incorporated herein.

78. The University and the Regents enabled Weiss to have access and use of electronic credentials that were his means of viewing and downloading personal, private, and intimate images and other confidential information of Plaintiffs and others similarly situated to them.

79. The Non-Individual Defendants failed to monitor, supervise, and review Weiss's activity, and failed to ensure his work duties were being undertaken and completed with respect for Plaintiffs' privacy and the privacy of others.

80. The Non-Individual Defendants failed to implement reasonable measures of security, failing to prove the most basic of security protection for the private information of student-athletes, including failing to consider or have multiple authentication credentials, background checks, peer reviews, or oversight.

81. The Non-Individual Defendants failed to implement reasonable protective measures to detect Weiss' irregular activity and insider hacking, including but not limited to, appropriate authentication tools, behavioral analytics, anomaly detection, machine learning, and real-time monitoring of user activity, looking for deviations from established patterns and suspicious actions like unusual login attempts or access to sensitive data, any of which would have prevented Weiss' improper access to private student information.

82. As a result of these failures, Weiss accessed private, intimate, and personal information pertaining to Plaintiffs and others similarly situated, all of which was maintained by Keffer, as encouraged and authorized for collection by the University and the Regents.

83. The careless and negligent misconduct of the Non-Individual Defendants in these respects enabled Weiss to target female college athletes to obtain their private and sensitive information without authorization, including but not limited to Plaintiffs.

84. The Non-Individual Defendants knew that Weiss had an advantage over others, by means of his job responsibilities, and would be able to access the private information and privacy interests of the Plaintiffs and their peers.

85. Because the Non-Individual Defendants failed to undertake reasonable security measures, he was enabled to freely research, target, and invade the privacy of various University athletes, particularly female athletes, who were targeted based on their school affiliation, athletic history, and physical attributes.

86. The failure of the Non-Individual Defendants to review Weiss' conduct, assess his credentials, monitor his work, or ensure oversight, left him free to prey on Plaintiffs and others, all without reporting what he was doing in furtherance of his duties. As such, Weiss was able to execute his goal of obtaining private photographs and videos of Plaintiffs and others that were never intended to be shared beyond Plaintiffs' intimate partners, and likewise for other victims similarly situated to the Plaintiffs.

87. Due to the recklessness of the University and the Regents, and the gross negligence/negligence of Keffer, Weiss downloaded personal, intimate digital photographs and videos of Plaintiffs and others, all of which Plaintiffs and class members entrusted to the Non-Individual Defendants.

88. Because the Non-Individual Defendants negligently and recklessly failed to exercise any reasonable control over Weiss, in the course of his employment with the University, Weiss was able to successfully target athletes such as Plaintiffs and others similar to them and download, obtain, and use their private and sensitive information and media.

89. Because the Non-Individual Defendants negligently and recklessly failed to monitor Weiss, he was able to compile records on individuals whose media he wanted, all of which he obtained, and then viewed.

90. The information that the Non-Individual Defendants permitted Weiss to obtain is highly private, secretive, embarrassing, and distressing when shared without authorization, and humiliating for it to be seen without authorization.

91. Weiss obtained access—without and in excess of his authorization—to personal and confidential student-athlete information and databases of more than 100 colleges and

universities across the country that were maintained by Keffer including but not limited to those of university athletes like Plaintiffs.

92. Thousands of students still remain at risk because the Non-Individual Defendants have failed to undertake any review of how Plaintiffs' private and personal information is stored, maintained, and who can access such information, and from where.

93. Upon information and belief, the University and the Regents also failed to properly investigate Keffer, Keffer's protocols, and failed to adequately monitor or establish safeguards for Keffer's work with the students and their private images to ensure they carried out their duties to safeguard and protect the private information entrusted to them.

94. The University and the Regents also failed to properly consider and/or implement ways to prevent and shield students from Weiss' misconduct.

95. Neither the University nor the Regents have provided an explanation as to why they failed to adequately undertake any review of the contract with Keffer, investigate Keffer, monitor or establish safeguards for Keffer's work with the students and their private images, or otherwise considered what action they should have taken to prevent this unauthorized access by Weiss.

96. Weiss, due to the lack of control and enabling from the Non-Individual Defendants, obtained unauthorized access to databases containing highly sensitive and private information of the Plaintiffs and others.

97. Upon information and belief, many, if not all, of the databases at issue are maintained by Keffer and were relied on by Plaintiffs to be securely safeguarded.

98. Plaintiffs and others similarly situated entrusted the University and the Regents to ensure Keffer protected their private information and images.

99. The Non-Individual Defendants failed to implement any reasonable action that would have protected Plaintiffs' private information from unauthorized access by Weiss.

100. Upon information and belief, exploiting these unsecured databases, Weiss downloaded personally identifiable information (PII) and medical records of more than 150,000 student-athletes, including Plaintiffs.

101. Upon information and belief, Weiss also downloaded passwords that athletes used to access Keffer's computer system to view and update their data, including that of Plaintiffs.

102. The athletes' passwords that Weiss downloaded were encrypted, but poorly secured because of the Non-Individual Defendants' recklessness so that Weiss, while not being monitored or supervised by the Non-Individual Defendants, managed to crack the encryption, using basic internet research.

103. Through open-source information, Weiss conducted additional targeted research on athletes such as Plaintiffs and obtained personal information such as their mothers' maiden names, pets, places of birth, and nicknames, all of which they had entrusted to Non-Individual Defendants to keep private and none of which the Non-Individual Defendants actually properly safeguarded.

104. Upon information and belief, using a combination of data obtained from the student-athlete databases and his internet research, based on the lack of supervision or monitoring by the Non-Individual Defendants, despite the foreseeability of such breaches as well as their responsibility to prevent and mitigate such breaches, Weiss was able to obtain access to the social media, email, and/or cloud storage accounts of more than 2,000 targeted athletes including but not limited to Plaintiffs and those similarly situated.

105. Once Weiss obtained access to the accounts of targeted athletes, he searched for and downloaded private, personal, and intimate media that were not publicly shared.

106. Upon information and belief, Weiss also obtained unauthorized access to the social media, email, and/or cloud storage accounts of more than 1,300 additional students and/or alumni from universities and colleges from around the country including, but not limited to Plaintiffs, as a result of the Non-Individual Defendants reckless disregard for their safety and personal privacy.

107. Once Weiss gained access to the accounts, he extracted personal, private, and intimate media.

108. The Non-Individual Defendants each took no reasonable actions to prevent this foreseeable and unauthorized access.

109. The Non-Individual Defendants have failed to take any reasonable steps to remedy the harm caused by the privacy violations they permitted to occur, and they have not contacted Plaintiffs or other affected student-athletes that they know or may have known had their privacy violated at the hands of Weiss.

110. Upon information and belief, Weiss exploited weaknesses in account authentication of Plaintiffs and others similarly situated to further gain access to accounts of students and alumni allowing him to infiltrate even more social media, email, and cloud storage accounts.

111. The Non-Individual Defendants have long been on notice that this kind of information Weiss accessed was expected to be kept private, would be embarrassing if accessed by third parties, and any breach would cause significant harm. Despite this, they failed to implement appropriate safeguards.

112. Weiss unlawfully obtained digital photographs, videos, and other private data belonging to more than 3,300 individuals including but not limited to Plaintiffs in of the course of his employment, and his misconduct and the misconduct of the Non-Individual Defendants were violations of Michigan and other state privacy laws.

113. From approximately 2021 to 2023, Weiss, in the course of his employment, unlawfully transferred, possessed and used, without lawful authority, information, images, and other media of Plaintiffs and others.

114. From approximately 2020 to 2021, Weiss intentionally accessed—as a result of the Non-Individual Defendants’ failure to protect the privacy of Plaintiffs and others—computers, networks, and information relating to Plaintiffs and others that was private in nature.

115. Weiss then, unlawfully, and under negligent supervision or monitoring by the Non-Individual Defendants, downloaded personally identifiable information and other medically protected information and medical records of more than 150,000 athletes including but not limited to Plaintiffs, all in violation of Michigan and other state privacy laws.

116. Upon information and belief, the United States Department of Justice is in the process of notifying thousands of potential victims that their privacy was breached..

117. Jane Doe 10 and Jane Doe 11 have already received such a notice from the United States Department of Justice.

118. As a direct result of the negligence, recklessness, and misconduct of the Defendants, Plaintiffs and those similarly situated have incurred substantial monetary and emotional damages exceeding \$50,000,000, exclusive of costs, interest, and fees.

CLASS ALLEGATIONS

119. Plaintiffs file this lawsuit both individually and as representatives of all others similarly situated pursuant to Fed. R. Civ. P. 23 on behalf of the following Class:

All student athletes whose personal data, images, information, social media, or videos were accessed by Weiss without authorization (the “Class Members”).

120. In addition, Plaintiffs believe a subclass may be appropriate for all class members who receive notice from the United States Department of Justice as to the likely violation of their privacy and rights by Weiss. Therefore, Plaintiffs plead a subclass as follows:

All student athletes whose personal data, images, information, social media, or videos were accessed by Weiss without authorization and who received a notice letter from the United States Department of Justice as to Weiss (the “DOJ Letter Sub-Class”).

121. Excluded from the Class are: (a) Defendant and any entity or division in which Defendant has a controlling interest, and their legal representatives, officers, directors, assigns, and successors; (b) the Judge to whom this case is assigned and the Judge’s staff; and (c) the attorneys representing any parties to this Class Action.

122. Plaintiffs reserve the right to modify or amend the definition of the proposed class and/or sub-classes before the Court determines whether certification is appropriate.

Numerosity – Fed. R. Civ. P. 23(a)(1)

123. Law enforcement officials have disclosed the numbers of victims is significant and exceeds one thousand satisfying the numerosity requirement. Although the exact number of Class Members is uncertain at this time, it will certainly be ascertained through appropriate discovery, the number is great enough such that joinder is impracticable.

124. The members of the Class are so numerous and geographically disperse that individual joinder of all members is impracticable.

125. Similarly, Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

126. Class Members are readily identifiable from information and records in the possession of the federal and state authorities, the Regents, the University, and Keffer.

127. Electronic records maintained by the Non-Individual Defendants who conducted their own investigation can confirm the identification of Class Members.

Commonality and Predominance – Fed. R. Civ. P. 23(a)(2) and 23(b)(3)

128. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and the other Class Members. Similar or identical violations, practices, and injuries are involved, and the burden of proof to establish violations of those rights involve uniform, objective questions of fact and law, both for the prosecution and for the defense. *Young v. Nationwide Mut. Ins. Co.*, 693 F.3d 532, 542-543 (6th Cir. 2012); *Hicks v. State Farm*, 2019 WL 646044 (E.D. Ky. 2019) *aff'd* 965 F3d 452 (2020); *Speerly v. Gen. Motors, LLC*, 343 F.R.D. 493, 512-522 (E.D. Mich 2023).

129. The common questions of fact and law existing as to all Class Members predominate over questions affecting only individual class members. The evidence required to advance Plaintiffs' and Class Members' claims are the same, common to all; as is true of the evidence Defendants will likely rely upon in defense of this action. Thus, the elements of commonality and predominance are both met.

130. For example, establishing the facts of how, where, who, when, and through what means the invasions of Plaintiffs and other Class Members occurred are identical.

131. Defendants' actions, inactions, negligence, and recklessness apply commonly to all Plaintiffs and Class Members.

132. The downloads and invasions by Weiss and the improper conduct accessing private information through unsecure facilities without permission is common to all Class Members and has caused injury to the Plaintiffs and Class Members in common manners.

133. The Sixth Circuit has held that cases involving a course of conduct or standard in a statute favors a finding of predominance "because the defendant's liability to all class members turned on whether it violated the applicable federal statute, not whether any individual customer requested the wire-maintenance program." *Beattie v. CenturyTel, Inc.*, 511 F.3d 554, 566 (6th Cir. 2007); *Hicks v. State Farm Fire & Cas. Co.*, 965 F.3d 452, 462 (6th Cir. 2020). Liability will be tested under the same standard, equally applicable for all class members, making certification appropriate under Rule 23(b)(3).

134. The majority of legal and factual issues of the Plaintiffs and the Class Members predominate over any individual questions, including:

- (a) Whether the Non-Individual Defendants implemented policies and practices to, and in fact did, supervise, monitor and investigate Weiss and Keffer adequately; secure media and other personal and sensitive information; allocate resources to preventing security breaches;
- (b) Whether the Non-Individual Defendants lack of control enabled unauthorized access to databases containing highly sensitive and private information of the Plaintiffs and others;
- (c) Whether Non-Individual Defendants are responsible and liable for the actions of Weiss and Keffer;
- (d) Questions of law relative to liability, including the constitutional and statutory provisions pleaded, and defenses to same;
- (e) Questions of media and digital security, including standards, applicable to Non-Individual Defendants;

- (f) Which years of activity are actionable; and
- (g) Other common questions of fact and law relative to this case that remain to be discovered.

135. Resolving the claims of these Class Members in a single action will provide benefit to all parties and the Court by preserving resources, avoiding potentially inconsistent results, and providing a fair and efficient manner to adjudicate the claims.

Commonality:

136. Predominance does not require Plaintiffs to prove an absence of individualized damage questions, or even proof of class wide damage in the aggregate. *Kuchar v. Saber Healthcare Holdings LLC*, 340 F.R.D. 115, 123 (N.D. Ohio 2021) (finding individualized damages questions also do not defeat a predominance finding and noting “when adjudication of questions of liability common to the class will achieve economies of time and expense, the predominance standard is generally satisfied even if damages are not provable in the aggregate.”)(citing *Hicks*, 965 F.3d at 460).

Typicality – Fed. R. Civ. P. 23(a)(3)

137. This test “limit[s] the class claims to those fairly encompassed by the named plaintiffs’ claims.” *In re American Med. Sys., Inc.*, 75 F.3d 1069, 1082 (6th Cir.1996) (citation and quotation omitted). The named class representatives meet the criteria for typicality.

138. Typicality does not mean the same claims or facts. *Senter v. General Motors Corp.*, 532 F.2d 511, 525 n. 31 (6th Cir. 1976), *cert. denied*, 429 U.S. 870, 97 S.Ct. 182, 50 L.Ed.2d 150 (1976): “[t]o be typical a representative’s claim need not always involve the same facts or law, provided there is a common element of fact or law.”

139. Here, typicality requires class representatives who, in their status as student athletes, were subject to the same common university rules, policies, practices and conduct.

140. Plaintiffs claims are typical of the Class Members because they are highly similar and the same and related in timing, circumstance, and harm suffered. To be sure, there are no defenses available to Defendants that are unique to individual Plaintiffs. The injury and causes of actions are common to the Class as all arising from the same statutory and privacy interests.

141. Defendants cannot merely raise speculation as an argument against certification, but rather, they must demonstrate the likelihood of any such defenses actually applying to class member claims. *Fox v. Saginaw County*, 67 F.4th 284, 301 (6th Cir. 2023).

142. The Supreme Court requires more than Defendants can provide in this regard. In *Halliburton Co. v. Erica P. John Fund, Inc.*, 573 U.S. 258, 276 (2014) the Supreme Court concluded that so long as plaintiffs could show that their evidence is capable of proving the key elements to plaintiffs' claim on a class-wide basis, the fact that the defendants would have the opportunity at trial to rebut that presumption as to some of the plaintiffs did not raise individualized questions sufficient to defeat predominance. "That the defendant might attempt to pick off the occasional class member here or there through individualized rebuttal does not cause individual questions to predominate." *Id.*

143. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

144. The need to conduct additional post certification stage discovery, such as further file review or class member surveys, to eliminate uninjured persons after trial, does not act as a *de facto* bar to certification. *Nixon*, 2021 WL 4037824, at *8 (citing *Young*, 693 F.3d at 540); *In re Visa Check/MasterMoney Antitrust Litig.*, 280 F.3d 124, 145 (2d Cir. 2001); *Perez v. First Am. Title Ins. Co.*, 2009 WL 2486003, at *7 (D. Ariz. Aug. 12, 2009) ("Even if it takes a substantial

amount of time to review files and determine who is eligible for the [denied] discount, that work can be done through discovery.”); *Slapikas v. First Am. Title Ins. Co.*, 250 F.R.D. 232, 250 (W.D. Pa. 2008) (finding class action manageable despite First American's assertion that “no database exists easily and efficiently to make the determination that would be required for each file”).

145. Any remaining disputes on membership or class members damages can be left to a special master's decision. *Whitlock v. FSL Mgmt., LLC*, 2012 WL 3274973, at *12 (W.D. Ky., 2012), *aff'd*, 843 F.3d 1084 (6th Cir. 2016). By placing the validation of injury step at the end of the class trial process, no injured class members are left out, and at the same time, Defendants are not at risk for paying any uninjured class members.

Adequacy of Representation – Fed. R. Civ. P. 23(a)(4)

146. Plaintiffs will adequately represent the class. They have no interests that are in conflict with those of the class. In addition, they have retained counsel competent and experienced in complex class action litigation, and they will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiffs and their counsel.

Superiority of Class Treatment – Fed. R. Civ. P. 23(b)(3)

147. The class action is superior to any other available procedures for the fair and efficient adjudication of these claims, and no unusual difficulties are likely to be encountered in the management of this class action.

148. The superiority analysis required to certify a class is designed to achieve economies of time, effort and expense, and to promote uniformity of decisions as to persons similarly placed, without sacrificing procedural fairness or bringing about other undesirable results. *Martin v. Behr-Dayton Thermal Parts LLC*, 896 F.3d 405, 415 (6th Cir. 2018) (citing *Amchem Prods v. Windsor*, 521 U.S. 591, 615 (1997)).

149. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable.

150. It would be an unnecessary burden upon the court system to require these individuals to institute separate actions. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

151. Pursuing this matter as a class action is superior to individual actions because:

- a. Separate actions by Class Members could lead to inconsistent or varying adjudications that would confront Defendants with potentially incompatible standards of conduct;
- b. Many victims will not come forward without a certified class;
- c. Final equitable relief will be appropriate with respect to the entire Class as a whole for monitoring, protection, therapy and other equitable forms of relief that may be provided;
- d. This action is manageable as a class action and would be impractical to adjudicate any other way;
- e. Absent the class action, individual Class Members may not know if their privacy was invaded; where such images are currently being stored, or are accessible by others; and their injuries are likely to go unaddressed and unremedied; and,
- f. Individual Class members may not have the ability or incentive to pursue individual legal action on their own.

Particular Issues – Fed. R. Civ. P. 23(c)(4)

152. In the event unforeseen issues preclude class certification under Fed.R.Civ.P. 23(b)(3), the case is still appropriate for class certification under Fed.R.Civ.P. 23(c)(4), as to the particular issues of liability.

153. Defendants have acted or refused to act on grounds generally applicable to Plaintiffs and the other members of the Class, thereby making declaratory relief, as described below, with respect to the Class as a whole.

**COUNT I – VIOLATION OF THE COMPUTER FRAUD AND
ABUSE ACT – 18 U.S.C. § 1030**

(Defendants Weiss, University and Regents)

154. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

155. Plaintiffs allege that Defendants Weiss, the University, and the Regents violated the Computer Fraud and Abuse Act.

156. Weiss violated the Computer Fraud and Abuse Act by unlawfully accessing, Plaintiffs' private information.

157. Weiss did so in connection with his job duties at the University.

158. Weiss' actions constituted a violation of the Act because he "intentionally accesse[d] a computer without authorization" and/or "exceed[ed] authorized access, and thereby obtain[ed] ... information." 18 U.S.C. § 1030(a)(2)(C).

159. Under the law, Weiss is considered an "inside hacker" since he accessed a computer system with permission as part of his employment that dealt with Plaintiffs and the Class Members as student athletes, however, Weiss in connection with and furtherance of his job duties, then exceeded the parameters of authorized access by entering an area of computerized network of information that was off-limits.

160. This situation can be compared to opening your office door to discover an unauthorized individual inside. If the person is a stranger with no right to be in the building, they lack authorization. If the person is a coworker, they may have exceeded their authorized access.

161. Weiss's actions were deliberate because he knew he was unauthorized and proceeded nevertheless and did so with the implicit approval from the University.

162. The University is vicariously liable for his actions because he conducted them while performing his role as a sports employee of the University's athletic department.

163. Legal precedent establishes that an employer is responsible for the wrongful acts committed by its employees in the course of their employment.

164. Under 18 U.S.C. § 1030(g), Plaintiffs may recover damages in this civil action from Weiss and the University along with injunctive relief or other equitable relief.

165. Given the willful violations committed by Weiss and the University, resulting in significant damage, harm, humiliation, and distress to Plaintiffs and other Class Members, Plaintiffs should be awarded all appropriate damages in this matter.

COUNT II – VIOLATIONS OF THE STORED COMMUNICATIONS ACT –
U.S.C. § 2701 et seq

(Defendants Weiss, University and Regents)

166. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

167. Plaintiffs allege that Defendants Weiss, the University, and the Regents violated the Stored Communications Act.

168. The Stored Communications Act, 18 U.S.C. § 2701 et seq., prohibits the unauthorized access of web-based cloud storage and media accounts such as those at issue and other accounts hosted by Keffer that did and do, like for Plaintiffs, contain personal, private, and intimate information about and relating to Plaintiffs and others situated similar to Plaintiffs.

169. Specifically, under 18 U.S.C. § 2701(a), it is not lawful for any person to: (1) intentionally accesses without authorization a facility through which an electronic communication

service is provided; or (2) intentionally exceed an authorization to access that facility; and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system.

170. Plaintiffs' electronic information and communications were in electronic storage and clearly fall within the scope of the statute.

171. The information, messages, files, and media were accessed by Weiss without authorization, in connection with his role at the University.

172. Weiss's access without authorization in connection with his University job duties were deliberate.

173. There is no manner in which Plaintiffs' private information, messages, files, and media that is in issue could have been obtained without unauthorized access and would not have been obtained without unauthorized access had Weiss not been an employee of the University working in his athletic capacity for which the University hired and employed him.

174. Under Section 2707 of the Stored Communications Act, individuals may bring a civil action for the violation of this statute.

175. This law imposes strict liability on violators.

176. The statute provides that a person aggrieved by a violation of the act may seek appropriate relief including equitable and declaratory relief, actual damages or damages no less than \$1,000 punitive damages, and reasonable attorney's fee[s] and other litigation costs reasonably incurred according to 18 U.S.C. § 2707(b)-(c).

177. The University's and Weiss's access to Plaintiffs' private, personal, and intimate information, messages, files, and media constituted a violation of 18 U.S.C. § 2701(a).

178. The University and Weiss knew they did not have authority to access Plaintiffs' private, personal, and intimate information, messages, files, and media but did so anyway.

179. Their intentional misconduct led to multiple violations of the Stored Communications Act.

180. As a result of these violations, Plaintiffs have incurred significant monetary and nonmonetary damages as a result of these violations of the Stored Communications Act, and Plaintiffs seek appropriate compensation for their damages.

181. Under the statute, Plaintiffs should be granted the greater of (1) the sum of their actual damages suffered and any profits made by the University and Weiss as a result of the violations or (2) \$1,000 per violation of the Stored Communications Act.

182. Given these violations were deliberate, the Court should assess punitive damages against Defendants as well.

183. Plaintiffs should also be granted reasonable attorney fees and costs.

COUNT III – VIOLATION OF TITLE IX, 20 U.S.C. § 1681(A) *Et Seq.*

(Defendants University and Regents)

184. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

185. Plaintiffs allege that Defendants the University and the Regents violated Title IX, 20 U.S.C. § 1681(A) *et seq.*

186. The University receives federal financial support for its educational programs and is therefore subject to the provisions of Title IX of the Education Act of 1972, 20 U.S.C. § 1681(a), *et seq.*

187. Title IX mandates that “No person in the United States shall on the basis of sex, be ... subject to discrimination under any education program or activity receiving Federal financial assistance ...”

188. Each Plaintiff and Class Member is a “person” under the Title IX statutory language.

189. Weiss specifically targeted women in his unwanted invasions of privacy and his misconduct is discrimination on the basis of sex.

190. The University, under Title IX, is obligated to investigate allegations of sexual harassment.

191. The University was aware of the sensitive nature of the private and personal information of Plaintiffs to which Weiss was able to access given his role.

192. The University and Regents acted with deliberate indifference to sexual harassment by:

- a. Failing to protect Plaintiffs and others as required by Title IX;
- b. Neglecting to adequately investigate and address the complaints regarding the deeply sensitive information Plaintiffs provided;
- c. Failing to institute corrective measures to prevent Weiss from sexually harassing other students; and
- d. Failing to adequately investigate the other multiple acts of deliberate indifference.

193. The University and the Regents acted with deliberate indifference as their lack of response to the sexual harassment was clearly unreasonable in light of the known circumstances.

194. The University's failure to promptly and appropriately protect, investigate, and remedy and respond to the sexual harassment of women has effectively denied them equal educational opportunities at the University, including access to medical care and sports training.

195. At the time the Plaintiffs received some medical and/or athletic training services from the University, they did not know the Non-Individual Defendants failed to adequately consider their safety including in their engagement, hire, training, and supervision of Weiss.

196. As a result of the University's and the Regents' deliberate indifference, Plaintiffs have suffered loss of educational opportunities and/or benefits.

197. Plaintiffs have and incurred, and will continue to incur, attorney's fees and costs of litigation.

198. At the time of Defendants' misconduct and wrongful actions and inactions, Plaintiffs were unaware, and or with reasonable diligence could not have been aware, of Defendants' institutional failings with respect to their responsibilities under Title IX.

199. The Regents and the University maintained a policy and/or practice of deliberate indifference to protection of female student athletes.

200. Defendants' policy and/or practice of deliberate indifference to protection against the invasion of privacy for female athletes created a increased risk of sexual harassment.

201. Despite being able to prevent these privacy violations and acts of harassment, Defendants failed to do so.

202. Because of the Regents' and the University's policy and/or practice of deliberate indifference, Plaintiffs had their privacy invaded and were sexually harassed by Weiss.

203. Plaintiffs should be awarded all such forms of damages in this case for Regents' and the University's conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

COUNT IV – VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.
§ 1983 – UNREASONABLE SEARCH AND SEIZURE

(Defendant Weiss)

204. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

205. Plaintiffs allege Defendant Weiss violated their civil rights under 42 U.S.C. § 1983 and the Fourth Amendment of the U.S. Constitution.

206. Defendant Weiss, sued in his individual capacity, was a state employee at all times relevant to this action, and acted under color of state law to deprive Plaintiffs of their "rights, privileges or immunities secured by the Constitution and laws" of the United States, 42 U.S.C. § 1983, specifically their Fourth Amendment right to be free warrantless and unreasonable searches and seizures.

207. At the time of his actions giving rise to this case, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally searched and seized Plaintiffs' private information without their consent, without a warrant, without probable cause or reasonable suspicion, and without any lawful basis or justification, in violation of Plaintiffs' clearly established rights under the Fourth Amendment.

208. The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated"

209. It is well settled that the Fourth Amendment's protection extends beyond the sphere of criminal investigations. *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 755 (2010) (citing *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 530 (1967)).

210. “The [Fourth] Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government,” without regard to whether the government actor is investigating crime or performing another function.” *Id.* (quoting *Skinner v. Railway Labor Executives' Assn.*, 489 U.S. 602, 613–614 (1989)).

211. Plaintiffs had a reasonable and legitimate expectation of privacy in their private, personal, and intimate information and images.

212. Acting under color of law, Defendant Weiss violated Plaintiffs’ clearly established right not to have their private, personal, and intimate information and images. accessed, searched, viewed, and seized when he searched and seized Plaintiffs’ private, personal, and intimate information and images without a warrant, without reasonable suspicion, without probable cause, and without any lawful basis, justification or need to support such an intrusion on Plaintiffs’ reasonable and legitimate expectation of privacy in that information.

213. Defendant Weiss’s search and seizure of Plaintiffs’ personal information was per se unreasonable under the Fourth Amendment.

214. Defendant Weiss’ search and seizure of Plaintiffs’ private, personal, and intimate information and images was unjustified at its inception and was not related in scope to any circumstances that would justify the search and seizure in the first place.

215. Defendant Weiss is not entitled to qualified immunity because Plaintiffs’ rights under the Fourth Amendment not to have their personal information searched and seized by him without a warrant, without permission, and without any lawful basis or justification, was obvious

and clearly established when Weiss accessed Plaintiffs' private information, such that no reasonable person in Weiss's position would believe that the act of searching and seizing Plaintiffs' private information was lawful under the specific circumstances presented, and Weiss had fair warning under the law as it existed at the time of his actions that those actions obviously violated Plaintiffs' rights under the Fourth Amendment. See, e.g., *G.C. v. Owensboro Public Schools*, 711 F.3d 623 (6th Cir. 2013) (Holding that high school officials violated the Fourth Amendment by searching a student's cell phone and reading his text messages); see also *Brannum v. Overton County School Bd.*, 516 F.3d 489, 499 (Stating that "Some personal liberties are so fundamental to human dignity as to need no specific explication in our Constitution in order to ensure their protection against government invasion[.]" and holding that school officials violated Fourth Amendment by installing cameras to surreptitiously record students in locker rooms.)

216. As a direct and proximate result of Weiss's violation of Plaintiffs' Fourth Amendment rights, Plaintiffs have suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

217. Plaintiffs should be awarded all such forms of damages in this case for Weiss's conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

COUNT V -- VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.
§ 1983 -- DUE PROCESS/BODILY INTEGRITY

(Defendant Weiss)

218. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

219. Plaintiffs are alleging Defendant Weiss violated their civil rights under 42 U.S.C. § 1983 and the Fourteenth Amendment of the U.S. Constitution.

220. Defendant Weiss, sued in his individual capacity, was a state employee at all times relevant to this action, and acted under color of state law to deprive Plaintiffs of their "rights, privileges or immunities secured by the Constitution and laws" of the United States, 42 U.S.C. § 1983, specifically their Fourteenth Amendment equal protection right to be free from sexual harassment in an educational setting, and their Fourteenth Amendment due process right to be free from violation of bodily integrity. *West v. Atkins*, 487 U.S. 42, 49-50 (1988) (quoting *Lugar v. Edmondson Oil Co.*, 457 U.S. 922, 936 n. 18 (1982)).

221. At the time of the actions giving rise to this case, it was obvious, clearly established, and known to Weiss that the right to be free from sexual abuse at the hands of a state employee was protected by the Due Process Clause of the Fourteenth Amendment, such that he knew his actions in accessing Plaintiffs' Plaintiffs' private, personal, and intimate information and images violated Plaintiffs' fundamental right of due process. *Doe v. Claiborne Cnty., Tenn. By & Through Claiborne Cnty. Bd. of Educ.*, 103 F.3d 495, 506-07 (6th Cir. 1996) (Stating that "the Due Process Clause protects students against abusive governmental power as exercised by a school. To be sure, the magnitude of the liberty deprivation that sexual abuse inflicts upon the victim is an abuse of governmental power of the most fundamental sort; it is an unjustified intrusion that strips the very essence of personhood. If the "right to bodily integrity" means anything, it certainly encompasses the right not to be sexually assaulted under color of law. This conduct is so contrary to fundamental notions of liberty and so lacking of any redeeming social value, that no rational individual could believe that sexual abuse by a state actor is constitutionally permissible under the Due Process Clause.").

222. At the time of his actions giving rise to this case, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he

intentionally engaged in actions which violated Plaintiffs' right of bodily integrity, in violation of the Due Process Clause.

223. Weiss's actions were malicious, intentionally harmful, and were taken with deliberate indifference, and were so outrageous as to shock the contemporary conscience.

224. As a direct and proximate result of Weiss's violation of Plaintiffs' Fourteenth Amendment rights, Plaintiffs have suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

225. Plaintiffs should be awarded all such forms of damages in this case for Weiss's conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

COUNT VI – VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.
§ 1983 – EQUAL PROTECTION

(Defendant Weiss)

226. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

227. Plaintiffs are alleging Defendant Weiss violated their civil rights under 42 U.S.C. § 1983 and the Fourteenth Amendment of the U.S. Constitution.

228. Weiss's deliberate and intentional actions in accessing Plaintiffs' personal, private, and intimate images and information constituted sexual harassment and abuse because Weiss accessed Plaintiffs' highly sensitive, private, and personal information, data, and media for his own personal and sexual purposes.

229. At the time of the actions giving rise to this case, it was obvious, clearly established, and known to Weiss that the right to be free from gender discrimination, including sexual harassment and abuse at the hands of a state employee, was protected by the Equal Protection Clause of the Fourteenth Amendment, such that Weiss knew his actions in accessing Plaintiffs'

personal, private, and intimate images and information violated Plaintiffs' rights under the Fourteenth Amendment. *Fitzgerald v. Barnstable Sch. Comm.*, 555 U.S. 246, 257-258 (2009); see also *Daniels v. Board of Education*, 805 F.2d 203, 206-07 (6th Cir.1986); *Gutzwiller v. Fenik*, 860 F.2d 1317, 1325 (6th Cir. 1988); *Kitchen v. Chippewa Valley Sch.*, 825 F.2d 1004, 1012 (6th Cir. 1987).

230. At the time of his actions giving rise to this case, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally engaged in sexual harassment and sexual abuse, in violation of the Equal Protection Clause.

231. As a direct and proximate result of Weiss's violation of Plaintiffs' Fourteenth Amendment rights, Plaintiffs have suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

232. Plaintiffs should be awarded all such forms of damages in this case for Weiss's conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

COUNT VII -- VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.
§ 1983 -- DUE PROCESS/DEPRIVATION OF PROPERTY

(Defendant Weiss)

233. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

234. Plaintiffs are alleging Defendant Weiss violated their civil rights under 42 U.S.C. § 1983 and the Fourteenth Amendment of the U.S. Constitution.

235. Defendant Weiss, sued in his individual capacity, was a state employee at all times relevant to this action, and acted under color of state law to deprive Plaintiffs of their "rights, privileges or immunities secured by the Constitution and laws" of the United States, 42 U.S.C. §

1983, specifically their Fourteenth Amendment due process right to be free of deprivations of property without due process

236. At the time of the actions giving rise to this case, it was obvious, clearly established, and known to Weiss that the right not to be deprived of one's property without due process was protected by the Due Process Clause of the Fourteenth Amendment, such that he knew his actions in accessing and misappropriating Plaintiffs' private, personal, and intimate information and images violated Plaintiffs' fundamental right of due process.

237. Plaintiffs and others similarly situated had a protected property interest in their personal, private, intimate, and confidential information.

238. At the time of his actions giving rise to this case, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally engaged in actions which violated Plaintiffs' right not to be deprived of their personal property, in violation of the Due Process Clause.

239. Weiss' actions were malicious, intentionally harmful, and were taken with deliberate indifference, and were so outrageous as to shock the contemporary conscience.

240. As a direct and proximate result of Weiss' violation of Plaintiffs' Fourteenth Amendment rights, Plaintiffs have suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

241. Plaintiffs should be awarded all such forms of damages in this case for Weiss' conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

COUNT VIII – FAILURE TO TRAIN AND SUPERVISE UNDER 42 U.S.C. § 1983

(Defendants University and Regents)

242. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

243. Plaintiffs allege the University and the Regents failed to train and supervise Weiss properly under 42 U.S.C. § 1983.

244. The University and the Regents had the ultimate responsibility and authority to train and oversee their employees, agents, and/or representatives including Weiss and all faculty and staff regarding their duties toward students, faculty, staff and visitors.

245. The University and the Regents neglected to train and supervise their employees, agents, and/or representatives including Weiss and all faculty and staff, regarding the following duties:

- a. Recognizing, reporting, and preventing unauthorized invasions of privacy on campus;
- b. Providing diligent supervision of student athletes and other individuals, including Weiss;
- c. Investigating any and all privacy invasions committed by Weiss;
- d. Safeguarding all students, faculty, staff, alumni, and visitors on the University's campus premises;
- e. Maintaining a campus environment free from sexual harassment and invasions of privacy; and
- f. Properly training faculty and staff to be aware of their individual responsibility for creating and maintaining a safe environment.

246. The University and the Regents failed to adequately train coaches, trainers, medical staff, Weiss, and others regarding the aforementioned duties which led to violations of Plaintiffs' rights.

247. The lack of training was the result of Defendants' deliberate indifference toward the well-being of student athletes.

248. The University and the Regents failure to adequately train is the direct cause of Plaintiffs' injuries and those similarly situated.

249. As a result, the University and the Regents deprived Plaintiffs of rights secured by the Fourteenth Amendment to the United States Constitution in violation of 42 U.S.C. § 1983.

250. Plaintiffs should be awarded all such forms of damages in this case for the Regents' and the University's conduct that caused harm, humiliation, distress, and embarrassment to Plaintiffs and the Class.

COUNT IX – INVASION OF PRIVACY INTRUSION UPON SECLUSION

(Defendant Weiss)

251. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

252. Plaintiffs allege Defendant Weiss intentionally invaded Plaintiffs' privacy by intruding upon their seclusion.

253. Plaintiffs allege the University and the Regents are vicariously liable for Weiss invading Plaintiffs' privacy by intruding upon their seclusion.

254. Plaintiffs' personal social media files, videos, and other images were each in electronic storage and were intended to be kept private.

255. Weiss unlawfully accessed this information.

256. His actions were not authorized.

257. This information would not have been obtained absent the negligence and misconduct of the Defendants.

258. Plaintiffs never granted permission to such access.

259. Plaintiffs feel embarrassed, ashamed, humiliated, and distressed that their private information has been accessed by strangers and third parties.

260. Plaintiffs' social media data, images, and other media are private information.

261. Plaintiffs had the right to expect all this information would remain private.

262. The methods Weiss used to access such information was objectively unreasonable.

263. As a result of Weiss' actions, Plaintiffs have incurred significant monetary and nonmonetary damages as a result of Defendants' actions and request the appropriate damages.

COUNT X – GROSS NEGLIGENCE

(Defendants Weiss and Keffer)

264. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

265. Plaintiffs allege Defendants Weiss and Keffer were grossly negligent.

266. Plaintiffs entrusted the Regents and the University to ensure methods were undertaken to secure, safeguard, and protect against authorized access to their private information.

267. Keffer was entrusted to keep Plaintiffs' private information private.

268. Plaintiffs relied on Defendant Keffer to securely maintain their personal, private information and data.

269. Plaintiffs did not authorize access to such information, data, and media by Weiss.

270. Plaintiffs had a right to keep such information, data, and media private, and had a reasonable expectation that Defendant Keffer would do so.

271. Defendant Keffer had a duty to securely maintain the Plaintiffs and others similarly situated personal photographs, videos and digital data.

272. Defendant Keffer was grossly negligent and breached their duties owed to the Plaintiffs and those similarly situated by:

- a. Failing to securely maintain their database to prevent unauthorized access of personal and private information;
- b. Failing to implement reasonable protective measures to detect Weiss's unauthorized access and irregular activity, including, but not limited to appropriate authentication tools, behavioral analytics, anomaly detection, machine learning, and real-time monitoring of user activity;
- c. Failing to appropriately monitor for deviations from expected patterns and suspicious logins, including multiple failed attempts to access accounts, unusual log-in attempts, or repeated access to sensitive data;
- d. Failing to notify the Plaintiffs and other student-athletes that their personal, private data had been improperly accessed; and
- e. Other negligence to be discovered.

273. The information, data, and media could not have been accessed but for Keffer's negligence.

274. Had Defendant Keffer securely maintained Plaintiffs data, this would have prevented Weiss from improperly and unlawfully accessing the private information of Plaintiffs and those similarly situated.

275. It was foreseeable that the personal, sensitive information of young female athletes may be a target of hacking, as such, reasonable care required Keffer to have appropriate systems in place to prevent such hacking and alerting them to such activity so it could be immediately terminated and allowed to persist for years.

276. Plaintiffs are embarrassed, ashamed, humiliated, and mortified that their private information has been accessed by total strangers and third parties.

277. Keffer's failures and omissions to secure this private data was so reckless that it shows a substantial lack of concern for injuries to Plaintiffs and the Class.

278. The Plaintiffs' private and personal information, data, and media was accessed by Weiss unlawfully.

279. Weiss' actions were unlawful and grossly negligent.

280. Plaintiffs did not authorize access to such information, data, and media by Weiss.

281. Plaintiffs and those similarly situated have incurred significant monetary and nonmonetary damages as a result of Defendants' actions, and should be awarded damages accordingly.

COUNT XI – NEGLIGENCE

(Defendant Keffer)

282. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

283. Plaintiffs entrusted the Regents and the University to ensure methods were undertaken to secure, safeguard, and protect against authorized access to their private information.

284. Keffer was entrusted to keep Plaintiffs' private information private.

285. Plaintiffs relied on Defendant Keffer to securely maintain their personal, private information and data.

286. Plaintiffs did not authorize access to such information, data, and media by Weiss.

287. Plaintiffs had a right to keep such information, data, and media private, and had a reasonable expectation that Defendant Keffer would do so.

288. Defendant Keffer had a duty to securely maintain the Plaintiffs and others similarly situated personal photographs, videos and digital data.

289. Defendant Keffer breached their duties owed to the Plaintiffs and those similarly situated by:

- a. Failing to securely maintain their database to prevent unauthorized access of personal and private information;
- b. Failing to implement reasonable protective measures to detect Weiss's unauthorized access and irregular activity, including, but not limited to appropriate authentication tools, behavioral analytics, anomaly detection, machine learning, and real-time monitoring of user activity;
- c. Failing to appropriately monitor for deviations from expected patterns and suspicious logins, including multiple failed attempts to access accounts, unusual log-in attempts, or repeated access to sensitive data;
- d. Failing to notify the Plaintiffs and other student-athletes that their personal, private data had been improperly accessed; and
- e. Other negligence to be discovered.

290. The information, data, and media could not have been accessed but for Keffer's negligence.

291. Had Defendant Keffer securely maintained Plaintiffs data, this would have prevented Weiss from improperly and unlawfully accessing the private information of Plaintiffs and those similarly situated.

292. It was foreseeable that the personal, sensitive information of young female athletes may be a target of hacking, as such, reasonable care required Keffer to have appropriate systems in place to prevent such hacking and alerting them to such activity so it could be immediately terminated and allowed to persist for years.

293. Plaintiffs are embarrassed, ashamed, humiliated, and mortified that their private information has been accessed by total strangers and third parties.

294. Keffer's failures and omissions to secure this private data was so negligent that it shows a substantial lack of concern for injuries to Plaintiffs and the Class.

295. Plaintiffs and those similarly situated have incurred significant monetary and nonmonetary damages as a result of Defendants' actions, and should be awarded damages accordingly.

COUNT XII - TRESPASS TO CHATTELS

(Defendant Weiss)

296. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

297. Plaintiffs allege Defendant Weiss is guilty of trespass to chattels.

298. Plaintiffs allege the University and the Regents are vicariously liable for Weiss' trespass to chattels.

299. Weiss intentionally and unlawfully access Plaintiffs' private and personal data, information, and media, thereby wrongfully asserting control over and interfering with their sensitive data without authorization.

300. This unauthorized access and control was deliberate and carried out with malicious intent.

301. Plaintiffs and the Class have incurred significant monetary and nonmonetary damages as a result of Weiss's intentional misconduct.

302. Plaintiffs are entitled to exemplary damages as a result of these intentional and harmful act and interference with, and wrongful exercise of control over, their property.

COUNT XIII – VIOLATIONS OF MCL § 600.2919a

(Defendant Weiss)

303. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

304. Plaintiffs allege Defendant Weiss violated MCL § 600.2919a.

305. Plaintiffs allege the University and the Regents are vicariously liable for Weiss' violation of MCL § 600.2919a.

306. MCL § 600.2919a provides:

- a. (1) A person damaged as a result of either or both of the following may recover 3 times the amount of actual damages sustained, plus costs and reasonable attorney fees:
 - i) (a) Another person's stealing or embezzling property or converting property to the other person's own use.
 - ii) (b) Another person's buying, receiving, possessing, concealing, or aiding in the concealment of stolen, embezzled, or converted property when the person buying, receiving, possessing, concealing, or aiding in the concealment of stolen, embezzled, or converted property knew that the property was stolen, embezzled, or converted.
- b. (2) The remedy provided by this section is supplemental to any other legal or equitable right or remedy available.

307. Plaintiffs were damaged as a result of Weiss possessing, concealing, aiding the concealment of, stealing, and/or embezzling Plaintiffs' private and personal information and converting that information, those videos, and those images to Weiss' own use by using that information for his own purposes and benefit.

308. Under MCL § 600.2919a, Plaintiffs are entitled to recover three times actual damages, plus costs and reasonable attorney fees.

COUNT XIV – ASSAULT

(Defendant Weiss)

309. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

310. Plaintiffs allege Defendant Weiss assaulted Plaintiffs and those similarly situated.

311. Plaintiffs allege the University and the Regents are vicariously liable for Defendant Weiss' assault on Plaintiffs.

312. Weiss' conduct, in accessing Plaintiffs' and other Class Members' personal and private information as outlined above was intentional without consent, authorization, or any legal justification.

313. His conduct caused a reasonable apprehension of imminent harm onto Plaintiffs and others similarly situated.

314. As a result, Plaintiffs suffered severe damages and seek compensation as appropriate for these damages.

COUNT XV – INTENTIONAL INFLICTION OF EMOTIONAL DISTRESS

(Defendant Weiss)

315. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

316. Plaintiffs allege Defendant Weiss is guilty of intentional infliction of emotional distress on Plaintiffs.

317. Plaintiffs allege the University and the Regents are vicariously liable for Defendant Weiss' intentional infliction of emotional distress on Plaintiffs.

318. Weiss' conduct in accessing Plaintiffs' private and personal data, media, and information, as outlined above, was intentional.

319. Weiss' conduct was both extreme and outrageous.

320. Weiss' access of Plaintiffs' private and personal data, information, and media was not for any proper or authorized use.

321. Weiss' conduct caused severe emotional distress to Plaintiffs.

322. Plaintiffs suffered severe emotional distress and economic damage as a result of Weiss' intentional actions and as such Plaintiffs seek compensation as appropriate for these damages.

**COUNT XV – VIOLATION OF MICHIGAN IDENTITY THEFT
PROTECTION ACT – MCL 445.61 et. seq.**

(Defendants Weiss and Keffer)

323. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

324. Plaintiffs allege Defendants Weiss and Keffer violated the Michigan Identity Theft Protection Act.

325. Plaintiffs' personal and private media, content, data, and information were stored electronically and intended to be kept private.

326. Weiss unlawfully accessed this private and personal information, data, and media.

327. His actions were not authorized.

328. Keffer maintained a database of Plaintiffs' sensitive information.

329. Keffer had a duty to notify Plaintiffs of the unauthorized breach of their very private data.

330. Defendants failed to notify Plaintiffs of such.

331. As a result, Plaintiffs and others similarly situated were unaware for years that their very sensitive data was being accessed without their permission or authorization in violation of Michigan's Identity Theft Protection Act.

332. As a result of Defendants' conduct, Plaintiffs suffered significant and severe damages and as such Plaintiffs seek compensation as appropriate for these damages.

RELIEF

WHEREFORE, Plaintiffs pray this Court grant the following relief:

- a. Enter a judgment encompassing the relief requested above, plus significant compensatory damages exceeding \$50,000,000.00 together with costs, interest and attorney fees, against Defendants, and such other relief to which they are entitled;
- b. An order certifying the proposed Class and Subclasses; designating Plaintiffs as the named representatives of the respective Class Members; and appointing their counsel as Class Counsel;
- c. All such equitable relief as the Court deems proper and just, including but not limited to, declaratory relief;
- d. Enter judgment in favor of Plaintiffs and against Defendants for treble the amount of the Surplus Proceeds plus actual attorney fees for violation of MCL 600.2919a;
- e. Award Plaintiffs costs, attorney fees as well as interest from the date of Judgment until paid; and
- f. Grant such further relief as is agreeable to equity and good conscience.

JURY DEMAND

For all triable issues, a jury is hereby demanded.

Respectfully Submitted,

SOMMERS SCHWARTZ, P.C.

By: /s/ Lisa M. Esser

Lisa M. Esser (P70628)

Richard L. Groffsky (P32992)

Jason J. Thompson (P47184)

Matthew G. Curtis (P37999)

Attorneys for Plaintiff

One Towne Square, 17th Floor

Southfield, MI 48076

(248) 355-0300

LEsser@sommerspc.com

rgroffsky@sommerspc.com

JThompson@sommerspc.com

MCurtis@sommerspc.com

Megan Bonanni (P52079)

Kevin M. Carlson (P67704)

Beth M. Rivers (P33614)

Danielle Y. Canepa (P82237)

Attorneys for Plaintiffs

117 W. Fourth Street, Suite 200

Royal Oak, MI 48067

(248) 398-9800

mbonnani@pittlawpc.com

kcarlson@pittlawpc.com

brivers@pittlawpc.com

dcanepa@pittlawpc.com

Dated: April 2, 2025

LAW OFFICES
SOMMERS SCHWARTZ, P.C.

CLOSED, reassigned

**U.S. District Court
Eastern District of Michigan (Detroit)
CIVIL DOCKET FOR CASE #: 2:25-cv-10870-MAG-EAS**

****CASE CLOSED ALL ENTRIES MUST BE MADE IN 25-cv-10806.**** Roe CLF 001 v. Weiss et al

Assigned to: District Judge Mark A. Goldsmith

Referred to: Magistrate Judge Elizabeth A. Stafford

Demand: \$9,999,000

Cause: 28:1332 Diversity-Personal Injury

Date Filed: 03/27/2025

Date Terminated: 05/23/2025

Jury Demand: Plaintiff

Nature of Suit: 360 P.I.: Other

Jurisdiction: Diversity

Plaintiff

Jane Roe CLF 001

represented by **Bryan Paul Thompson**
Clarkson Law Firm, P.C.
875 North Michigan Avenue
31st Floor
Chicago, IL 60611
312-267-0061
Email: bthompson@clarksonlawfirm.com
ATTORNEY TO BE NOTICED

Yana A. Hart
Clarkson Law Firm
22525 Pacific Coast Highway
Malibu, CA 90265
213-788-4050
Email: yhart@clarksonlawfirm.com
ATTORNEY TO BE NOTICED

Ryan Clarkson
Clarkson Law Firm, P.C.
Clarkson Law Firm, P.C.
22525 Pacific Coast Highway
Malibu, CA 90265
213-788-4050
Email: rclarkson@clarksonlawfirm.com
ATTORNEY TO BE NOTICED

V.

Defendant

Matthew Weiss

Defendant

University of Michigan

represented by **Daniel B. Tukel**
Butzel Long
201 West Big Beaver Road
Suite 1200
Troy, MI 48084

313-225-7047

Email: tukel@butzel.com

*ATTORNEY TO BE NOTICED***Sheldon H. Klein**

Butzel

201 West Big Beaver Road

Suite 1200

Troy, MI 48084

248-258-1414

Fax: 248-258-1439

Email: klein@butzel.com

*ATTORNEY TO BE NOTICED***Defendant****Regents of the University of Michigan**represented by **Daniel B. Tukel**

(See above for address)

*ATTORNEY TO BE NOTICED***Sheldon H. Klein**

(See above for address)

*ATTORNEY TO BE NOTICED***Defendant****Keffer Development Services, LLC**represented by **Carl Andrew Fejko**

Dillon McCandless King Coulter Graham

Civil Practice

128 West Cunningham St.

Butler, PA 16001

724-822-2148

Email: cfejko@dmkcg.com

*ATTORNEY TO BE NOTICED***Jordan P. Shuber**

Dillon McCandless King Coulter &

Graham, LLP

128 West Cunningham Street

Butler, PA 16001

724-283-2200

Fax: 724-283-2298

Email: jshuber@dmkcg.com

*ATTORNEY TO BE NOTICED***Thomas W. King , III**

Dillon McCandless King Coulter & Graham

LLP

128 West Cunningham Street

Buter, PA 16001

724-283-2200

Email: tking@dmkcg.com

ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
03/27/2025	<u>1</u>	COMPLAINT filed by Jane Roe CLF 001 against Keffer Development Services, LLC, Regents of the University of Michigan, University of Michigan, Matthew Weiss with Jury Demand. Plaintiff requests summons issued. Receipt No: AMIEDC-10175497 - Fee: \$ 405. County of 1st Plaintiff: Washtenaw - County Where Action Arose: Washtenaw - County of 1st Defendant: Washtenaw. [Previously dismissed case: No] [Possible companion case(s): E.D. Michigan - Southern Division, 2:25-cv-10806; 2:25-cv-10855, Judge Mark A. Goldsmith; Linda V. Parker] (Attachments: # <u>1</u> Exhibit Civil Cover Sheet) (Clarkson, Ryan) (Entered: 03/27/2025)
03/28/2025	<u>2</u>	SUMMONS Issued for *Keffer Development Services, LLC, Regents of the University of Michigan, University of Michigan, Matthew Weiss* (LHam) (Entered: 03/28/2025)
03/28/2025		A United States Magistrate Judge of this Court is available to conduct all proceedings in this civil action in accordance with 28 U.S.C. 636c and FRCP 73. The Notice, Consent, and Reference of a Civil Action to a Magistrate Judge form is available for download at http://www.mied.uscourts.gov (LHam) (Entered: 03/28/2025)
04/01/2025	<u>3</u>	ORDER REASSIGNING CASE from District Judge Jonathan J.C. Grey and Magistrate Judge Curtis Ivy, Jr to District Judge Mark A. Goldsmith and Magistrate Judge David R. Grand. (NAhm) (Entered: 04/01/2025)
04/07/2025	<u>4</u>	STIPULATED ORDER EXTENDING TIME TO RESPOND TO COMPLAINT UNTIL JUNE 5, 2025 - Signed by District Judge Mark A. Goldsmith. (CCie) (Entered: 04/07/2025)
04/08/2025	<u>5</u>	NOTICE of Appearance by Daniel B. Tukel on behalf of Regents of the University of Michigan, University of Michigan. (Tukel, Daniel) (Entered: 04/08/2025)
04/09/2025	<u>6</u>	ORDER OF RECUSAL AND REASSIGNING CASE from Magistrate Judge David R. Grand to Magistrate Judge Kimberly G. Altman. (NAhm) (Entered: 04/09/2025)
04/10/2025	<u>7</u>	CORRECTED ORDER OF RECUSAL AND REASSIGNING CASE from Magistrate Judge David R. Grand to Magistrate Judge Elizabeth A. Stafford. (NAhm) (Entered: 04/10/2025)
04/15/2025	<u>8</u>	NOTICE of Appearance by Sheldon H. Klein on behalf of Regents of the University of Michigan, University of Michigan. (Klein, Sheldon) (Entered: 04/15/2025)
04/15/2025	<u>9</u>	NOTICE by Jane Doe from 10806 (Attachments: # <u>1</u> Exhibit) (Stinar, Parker) Modified on 4/16/2025 (LHam). [NOTICE OF MOTION TO CONSOLIDATE WITH CASE 25-10806 AND NOTICE TO APPOINT LEAD COUNSEL] Modified on 4/16/2025 (LHam). (Entered: 04/15/2025)
04/16/2025	<u>10</u>	NOTICE by Regents of the University of Michigan, University of Michigan <i>of filing Motion to Consolidate in case 25-cv-10806</i> (Tukel, Daniel) (Entered: 04/16/2025)
04/22/2025	<u>11</u>	ORDER Regarding Status Conference. Signed by District Judge Mark A. Goldsmith. (HRya) (Entered: 04/22/2025)
04/22/2025	<u>12</u>	NOTICE TO APPEAR REMOTELY: Status Conference set for 5/14/2025 at 9:00 AM before District Judge Mark A. Goldsmith. (HRya) (Entered: 04/22/2025)
04/22/2025	<u>13</u>	WAIVER OF SERVICE Returned Executed. Keffer Development Services, LLC waiver sent on 4/22/2025, answer due 6/23/2025. (Clarkson, Ryan) (Entered: 04/22/2025)
04/23/2025	<u>14</u>	NOTICE by All Plaintiffs <i>of Filing Motion for Staus Conference</i> (Thompson, Jason) (Entered: 04/23/2025)

04/24/2025	15	NOTICE by Jane Doe from 10806 <i>Majority Plaintiffs' Amended Motion</i> (Stinar, Parker) (Entered: 04/24/2025)
04/28/2025	16	NOTICE of Appearance by Bryan Paul Thompson on behalf of Jane Roe CLF 001. (Thompson, Bryan) (Entered: 04/28/2025)
04/29/2025	17	NOTICE of Appearance by Yana A. Hart on behalf of Jane Roe CLF 001. (Hart, Yana) (Entered: 04/29/2025)
05/06/2025	18	NOTICE by All Plaintiffs re 14 Notice (Other) <i>Corrected Notice of Filing Motion for Status Conference</i> (Thompson, Jason) (Entered: 05/06/2025)
05/14/2025	19	NOTICE of Appearance by Thomas W. King, III on behalf of Keffer Development Services, LLC. (King, Thomas) (Entered: 05/14/2025)
05/14/2025		Minute Entry for remote proceedings before District Judge Mark A. Goldsmith: Status Conference held on 5/14/2025. (Court Reporter: None Present, Not on the Record) (JHea) (Entered: 05/14/2025)
05/14/2025	20	NOTICE of Appearance by Carl Andrew Fejko on behalf of Keffer Development Services, LLC. (Fejko, Carl) (Entered: 05/14/2025)
05/15/2025	21	NOTICE of Appearance by Jordan P. Shuber on behalf of Keffer Development Services, LLC. (Shuber, Jordan) (Entered: 05/15/2025)
05/16/2025	22	NOTICE by Jane Roe CLF 001 re: <i>Supplemental Memorandum in Support of Plaintiff Counsels Motion for Appointment of Interim Class Counsel</i> (Attachments: # 1 Exhibit A) (Hart, Yana) (Entered: 05/16/2025)
05/23/2025	23	ORDER FOR CONSOLIDATION AND RELATED MATTERS. Signed by District Judge Mark A. Goldsmith. (JHea) (Entered: 05/23/2025)
05/23/2025	24	Notice to Parties Regarding Consolidated Case: Order of consolidation entered on *5/23/2025*. Designated lead case number is *25-10806*. (JHea) (Entered: 05/23/2025)

PACER Service Center			
Transaction Receipt			
06/05/2025 16:35:25			
PACER Login:	ThomaKingtking	Client Code:	
Description:	Docket Report	Search Criteria:	2:25-cv-10870-MAG-EAS
Billable Pages:	4	Cost:	0.40

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION**

JANE ROE CLF 001, individually and on
behalf of all others similarly situated,

Plaintiff,

Case No.

vs.

Hon.

MATTHEW WEISS; THE REGENTS OF
THE UNIVERSITY OF
MICHIGAN; THE UNIVERSITY OF
MICHIGAN; KEFFER DEVELOPMENT
SERVICES, LLC,

Defendants.

/

CLARKSON LAW FIRM, P.C.

Ryan J. Clarkson (P68616)

rclarkson@clarksonlawfirm.com

Yana Hart (*Pro Hac Vice Forthcoming*)

yhart@clarksonlawfirm.com

Bryan P. Thompson (*Pro Hac Vice
Forthcoming*)

bthompson@clarksonlawfirm.com

22525 Pacific Coast Highway

Malibu, CA 90265

Tel: (213) 788-4050

Fax: (213) 788-4070

*Attorneys for Plaintiff and
the Putative Class*

/

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff Jane Roe CLF 001 (“Jane Roe”) individually and on behalf of all others similarly situated, (“Plaintiff”) brings this Action against Matthew Weiss (“Weiss”), The University of Michigan (“University”), the Board of Regents of the University of Michigan (“Regents”) (collectively with the University “University Defendants”), and Keffer Development Services, LLC (“Keffer”). Plaintiff’s allegations are based upon personal knowledge as to herself and her own acts, and upon information and belief as to all other matters based on the investigation conducted by and through Plaintiff’s attorneys. Plaintiff believes that substantial additional evidentiary support will exist for the allegations set forth below, after a reasonable opportunity for discovery.

INTRODUCTION

1. This class action stems from the University of Michigan’s failure to protect the safety and trust of its students—particularly female student-athletes—by enabling former football coach Matthew Weiss to abuse his position and access university systems to commit obscene privacy violations over an eight-year period, from 2015 to 2023.

2. Defendant Weiss was a prominent figure within the University’s athletic program. In the course of his employment, the University granted him access to information systems containing highly sensitive student data. The access granted was unduly broad. It was also unmonitored.

3. Over the course of eight years, Weiss exploited this unfettered access to download sensitive personal data on hundreds of thousands of students, if not more. He then used it to systemically hack into personal accounts of primarily female student-athletes, stealing highly intimate photos and private conversations for his own perverse use. Reports indicate Weiss targeted at least 150,000 student-athletes within the University and over 100 other universities.

4. These violations went undetected for nearly a decade due to the University's gross negligence in supervising employees and securing its student data systems. Despite leveraging its highly regarded athletics program to bolster its reputation and attract students, the University failed to implement even the most basic safeguards to protect the rights and privacy of its student-athletes.

5. Sadly, this is not the first time the University has been complicit in enabling a sexual predator within its athletics program. Roughly five years ago, it was confirmed that one of the program's most prominent doctors had molested student-athletes for decades. The University's failure to address that egregious misconduct resulted in a historic \$490 million settlement in 2022. But despite that resolution, the University took no meaningful action to review or improve its hiring, supervision, or oversight practices within the athletics department.

6. Weiss was able to exploit these systemic failures of supervision, compounded by the University's equally deficient data security measures. Neither

the University nor Defendant Keffer, its data systems vendor, properly monitored those systems for unauthorized activity or unusual access patterns.

7. Weiss' extensive data downloads of personal student data should have raised immediate red flags, had even basic monitoring protocols been in place. Instead, these failings enabled Weiss's predatory behavior to continue undetected for over eight years.

8. Universities are responsible for supervising their employees. They are responsible for securing their data systems. Most of all, they are responsible for the safety and well-being of their students. University of Michigan failed on all counts.

9. Hundreds of thousands of students and young women have been impacted by these life-altering events, with intimate aspects of their personhood and bodily integrity violated for almost a decade, amid an ongoing failure of the University even to notify impacted students. Court intervention is necessary to hold Weiss, the University, its Regents, and its vendor accountable for these tragic failures, and to ensure they never happen again. The University of Michigan may be world renowned for its academics as well as its athletics, but none of that matters if its students are not safe.

PARTIES

Plaintiff

10. Plaintiff Jane Roe¹ is a natural person and resident of the State of Michigan.

Defendants

11. Matthew Weiss is an individual who, on information and belief, resided in Michigan during all relevant times in this Complaint.

12. The University of Michigan is a public university organized under the laws of Michigan, and located in Ann Arbor, Michigan.

13. The Regents of the University of Michigan is the governing board of the University, and “shall constitute the body corporate, with the right, as such, of suing and being sued.” Mich. Comp. Laws § 390.3-§ 390.4.

14. Keffer Development Services, LLC is a Pennsylvania-based limited liability company registered to conduct business in Michigan with its principal place of business in Grove City, Pennsylvania, which does business nationwide, including throughout the State of Michigan.

¹ Given the significant privacy concerns at stake, Plaintiff respectfully requests permission to proceed pseudonymously and anticipates filing a Motion to Proceed Pseudonymously as necessary.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction of this action pursuant to 28 U.S.C. Section 1332(d) because this is a class action where the aggregate amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from one of the Defendants. This Court has supplemental jurisdiction over any state law claims pursuant to 28 U.S.C. Section 1367.

16. This Court has supplemental jurisdiction over any state law claims pursuant to 28 U.S.C. Section 1367. Furthermore, the Class Members reside nationwide.

17. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District: The University Defendants have their principal place of business in this District and Class Members were affected by the Defendants' actions and inactions directed from this District.

///

///

///

///

FACTUAL ALLEGATIONS

The University of Michigan

18. The University of Michigan is the largest public university and research institution in the state of Michigan, with 52,855 students enrolled in the fall of 2024.² The university was ranked #3 in National Public Universities by the U.S. News & World Report in 2024.³

19. The University of Michigan's athletics department is highly funded and has \$238,866,661 in operating revenues.⁴ The University of Michigan's athletics team, the Wolverines, comprises 29 varsity sports teams. The Wolverines football team recently won the 2023 national championship of the NCAA Division I Football Bowl Subdivision. Roughly 1,032 student athletes participate in varsity sports at the University of Michigan, 544 of whom are male and 488 are female.⁵

² *University reports record enrollment for fall 2024*, UNIVERSITY OF MICHIGAN (Sept. 26, 2024) [https://record.umich.edu/articles/u-m-reports-record-enrollment-for-fall-](https://record.umich.edu/articles/u-m-reports-record-enrollment-for-fall-2024/#:~:text=The%20University%20of%20Michigan%20continues,within%20the%20state%20of%20Michigan.)

[2024/#:~:text=The%20University%20of%20Michigan%20continues,within%20the%20state%20of%20Michigan.](https://record.umich.edu/articles/u-m-reports-record-enrollment-for-fall-2024/#:~:text=The%20University%20of%20Michigan%20continues,within%20the%20state%20of%20Michigan.)

³ *Facts and Figures*, UNIVERSITY OF MICHIGAN, <https://umich.edu/facts-figures/> (last accessed Mar. 26, 2025).

⁴ Tony Garcia, *Michigan athletic department had \$557K surplus for 2024 fiscal year with \$238M in revenue*, DETROIT FREE PRESS (Jan. 30, 2025), <https://www.freep.com/story/sports/college/university-michigan/wolverines/2025/01/30/michigan-athletic-department-revenue-2024/78054625007/>.

⁵ *University of Michigan - Ann Arbor Sports Information*, COLLEGE FACTUAL, <https://www.collegefactual.com/colleges/university-of-michigan-ann-arbor/student-life/sports/> (last accessed Mar. 26, 2025).

The University of Michigan Has Failed Its Students in The Past

20. The University of Michigan has failed their athletes in the past by failing to properly supervise and monitor their employees.

21. In 2022, the University of Michigan reached a \$490 million settlement in connection with the sexual abuse allegations involving the university's former sports team physician, Dr. Robert Anderson. At least 1,050 survivors came forward with accounts that Anderson molested or sexually abused them.⁶

22. While that may be the most prominent example of the University's failure to protect students from sexual predators, it is not the only one. For example, in 2022 two graduate students also came forward with allegations of sexual harassment and abuse perpetrated by Professor Robert Stephenson in the School of Nursing at the University of Michigan. The students filed a complaint with The University of Michigan's Equity, Civil Rights and Title IX Office (ECRT) alleging Stephenson sexually harassed them, including sending them sexually explicit text messages and inflicting physical sexual abuse over the course of several years.⁷ ECRT initially dismissed the evidence of sexual misconduct and concluded there

⁶ Ivan Pereira, *University of Michigan reaches \$490M settlement with sex abuse survivors*, ABC NEWS (Jan. 19, 2022), <https://abcnews.go.com/US/university-michigan-reaches-490m-settlement-sex-abuse-survivors/story?id=82353991>.

⁷ *ECRT finds Nursing Prof. Robert Stephenson violated sexual misconduct policy, fabricated evidence*, THE MICHIGAN DAILY (Dec. 5, 2023), <https://www.michigandaily.com/news/focal-point/ecrt-finds-nursing-prof-robert-stephenson-violated-sexual-misconduct-policy-fabricated-evidence/>.

was insufficient evidence to prove Stephenson violated the University's misconduct policy.

23. However, because the students appealed, a follow-up ECRT investigation was conducted, proving that Stephenson forged documentation and attempted to destroy incriminating evidence.⁸ The University's inadequate and incomplete response the first time failed these students, further re-traumatizing them in the process. These failures reveal "that the power hierarchies, culture, and organizational workings of the University of Michigan enable and normalize abuse."⁹

24. Another example of these systemic failures involved Martin Philbert, the former provost and chief academic officer. Philbert was the second-highest administrator at the University of Michigan—with a lengthy history of sexually harassing female employees and graduate students. In 2020, the University of Michigan reached a settlement of \$9.25 million settlement with eight women who were sexually harassed by Philbert.¹⁰

⁸ *Id.*

⁹ *Another Harassment Scandal at the University of Michigan, GRADUATE EMPLOYEES' ORGANIZATION* (June 7, 2023), <https://www.geo3550.org/2023/06/07/another-harassment-scandal-at-the-university-of-michigan/>.

¹⁰ David Jesse, *University of Michigan reaches \$9 million settlement with 8 women who were sexually harassed by ex-provost*, USA TODAY (Nov. 18, 2020) <https://www.usatoday.com/story/news/education/2020/11/18/university-michigan-martin-philbert-sexual-harassment-settlement/3764027001/>.

The Latest Tragedy

25. On March 20, 2025, former University of Michigan football Co-Offensive Coordinator, Matthew Weiss, was charged in a 24-count indictment alleging 14 counts of unauthorized access to computers and 10 counts of aggravated identity theft.¹¹

26. From approximately 2015 through at least January 2023, Matthew Weiss, while employed at the University of Michigan’s athletic department, acquired unauthorized access to the student athlete databases of more than 100 colleges and universities that were managed by a third-party vendor, Keffer Development Services. By compromising the passwords of accounts with elevated levels of access the University provided without oversight, Weiss was able to acquire access to these student athlete databases.¹²

27. After acquiring access to these databases, Weiss then downloaded the personally identifiable information (“PII”), medical data and personal health

¹¹ *Former University of Michigan Football Quarterbacks Coach and Co-Offensive Coordinator Indicted on Charges of Unauthorized Access to Computers and Aggravated Identity Theft*, UNITED STATES ATTORNEY’S OFFICE, (Mar. 20, 2025) <https://www.justice.gov/usao-edmi/pr/former-university-michigan-football-quarterbacks-coach-and-co-offensive-coordinator>.

¹² Indictment at 2, *United States of America v. Matthew Weiss*, No. 2:25-cr-20165 (E.D. Mich. Mar. 20, 2025), <https://www.justice.gov/usao-edmi/media/1394076/dl?inline>.

information (“PHI”) (collectively “Private Information”) of more than 150,000 student athletes.¹³

28. Due to Defendants’ poor cybersecurity measures, failure to limit access, and failure to oversee its employees and systems, Weiss was able to obtain download the encrypted passwords that athletes utilized to access Keffer Development Services’ system to view and update the athletes’ data by cracking the system’s inadequate encryption that was purportedly “protecting” the passwords, easily guided by research he conducted on the internet.¹⁴ Keffer’s failure to protect against this known vulnerability underscores its gross negligence.

29. Using the information he acquired from Keffer, in addition to information that he acquired through other sources, Weiss was able to obtain further unauthorized access to the social media, email, and/or cloud storage accounts of more than 2,000 target athletes as well as more than 1,300 students or alumni from schools across the country by guessing or resetting their passwords, unbeknownst to account holders.¹⁵

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *Former University of Michigan Football Quarterbacks Coach and Co-Offensive Coordinator Indicted on Charges of Unauthorized Access to Computers and Aggravated Identity Theft*, UNITED STATES ATTORNEY’S OFFICE EASTERN DISTRICT OF MICHIGAN (March 20, 2025), <https://www.justice.gov/usao-edmi/pr/former-university-michigan-football-quarterbacks-coach-and-co-offensive-coordinator>.

30. Weiss' research on targeted athletes included searching for personal information that might be pertinent to identifying their passwords, such as their mothers' maiden names, pets' names, places of birth, and nicknames.¹⁶

31. After obtaining access to the personal accounts of the targeted athletes, Weiss searched for and downloaded the personal, intimate digital photographs and videos of these account holders, which were never intended to be shared with anyone other than their intimate partners.¹⁷

32. Beyond gaining unauthorized access to the personal, intimate digital photographs and videos of targeted athletes, which were not intended for public viewing, Weiss kept notes on these individuals, who consisted primarily of female college athletes, including notes commenting on their bodies and sexual preferences—all unbeknownst to them.¹⁸

¹⁶ Indictment at 2-3, *United States of America v. Matthew Weiss*, No. 2:25-cr-20165 (E.D. Mich. Mar. 20, 2025), <https://www.justice.gov/usao-edmi/media/1394076/dl?inline>.

¹⁷ *Former University of Michigan Football Quarterbacks Coach and Co-Offensive Coordinator Indicted on Charges of Unauthorized Access to Computers and Aggravated Identity Theft*, UNITED STATES ATTORNEY'S OFFICE EASTERN DISTRICT OF MICHIGAN (March 20, 2025), <https://www.justice.gov/usao-edmi/pr/former-university-michigan-football-quarterbacks-coach-and-co-offensive-coordinator>.

¹⁸ Indictment at 2, *United States of America v. Matthew Weiss*, No. 2:25-cr-20165 (E.D. Mich. Mar. 20, 2025), <https://www.justice.gov/usao-edmi/media/1394076/dl?inline>.

33. Sometimes, Weiss returned years later to search for new images of these targeted individuals, who he researched and sought out based on their school affiliation, athletic history, and physical characteristics.¹⁹

34. During Weiss' almost decade-long crime spree, the University of Michigan, its Board of Regents, and Keffer Development, which created and maintained the cloud software Weiss used to obtain Private Information for over 150,000 student athletes, gave Weiss unnecessary access to vast amounts of personal information and allowed him to exfiltrate it for his own use. There were no checks in place to monitor Weiss' access and use of data or to detect the highly unusual activity. This also enabled Weiss to hack into personal accounts of thousands of students, student athletes, and alumni to violate intimate aspects of their personhood and bodily integrity for almost a decade.

Jane Roe's Experience

35. Jane Roe is a junior at the University of Michigan, Ann Arbor campus, and has been active in the athletics program there since she enrolled.

¹⁹ *Former NFL, Michigan assistant coach Matt Weiss charged with hacking for athletes' intimate photos*, AP NEWS (Mar. 20, 2025) <https://apnews.com/article/michigan-football-college-coach-hacking-weiss-2f57fd02043b1cac114b209b1d6a4c>.

36. Plaintiff Roe was one of the student athletes whose information was unlawfully obtained, without authorization, by Weiss for his own personal use and without Plaintiff's knowledge or agreement.

37. Plaintiff Roe's personal information is still being held by the University Defendants and Keffer, and thus could still be potentially misused by bad actors such as Weiss.

38. Plaintiff Roe would not have consented to Defendant Weiss obtaining her Private Information for his own personal use if she had been given the opportunity to consent.

39. Plaintiff Roe did not know, and could not have reasonably known, that Defendant Weiss would secretly obtain, view, exfiltrate, or use her Private Information for his own illicit use.

40. Plaintiff Roe did not know, and could not have reasonably known, that the University Defendants would fail to properly screen, vet, hire, supervise, or discipline their employees, including Weiss, to the degree that he was able to invade her privacy and that of thousands of other student athletes.

41. Plaintiff Roe did not know, and could not have reasonably known, that Keffer would fail to properly secure her Private Information and prevent individuals like Weiss from obtaining her Private Information without her knowledge or consent.

42. Plaintiff Roe would not have provided her information to Keffer or the University Defendants if she had known they would fail to adequately protect her Private Information from accused criminals like Weiss.

43. Plaintiff Roe believed that the University would ensure its employees, including Weiss, followed all applicable laws and regulations and would not attempt to secretly or illegally obtain her Private Information, or that of other students or student athletes.

44. Plaintiff Roe believed that any technology vendor or contractor for the University, like Keffer, would ensure her information was secure from theft, exfiltration, or illicit use.

45. Plaintiff Roe was shocked and appalled when she found out, through the media and public filings, that Weiss had illegally obtained her Private Information for his own personal use. Plaintiff Roe felt violated, humiliated, and suffered an invasion of privacy that cannot be remedied.

46. Plaintiff seeks to hold the Defendants accountable for their actions and inactions that have caused immense fear, anxiety, humiliation, loss of dignity, and loss of privacy that cannot simply be undone. Plaintiff and the Class Members seek not just compensation, but also injunctive and equitable relief to ensure this failure is the last.

///

Loss of Privacy and Dignitary Harm

47. Defendants' conduct enabled a significant violation of privacy, extending far beyond the mere loss of data. The type of information compromised ranged from personal information like names, contact information and passwords to medical and psychological information and intimate photos and communications that were never meant for public viewing or viewing by an unauthorized third party. When extremely sensitive personal information such as this is compromised, individuals face a cascade of potential harm that erodes their sense of security and control, as information that they thought would remain confidential and private has now been leaked to the outside world, and which they no longer exercise control over. This exposure can lead to a profound sense of vulnerability, as individuals grapple with the knowledge that their most personal details are now in the hands of unknown actors, free to circulate and be publicized now, or at any time in the future.

48. Information regarding an individual's health and medical choices, such as here, as well as private communications and intimate photos meant for a romantic partner are among the most sensitive information there is. An individual's right to privacy regarding their body, their medical and psychological care, their romantic interests and their sexual and intimate life are the most sacrosanct and inviolable rights an individual possesses, striking to the very core of their personhood and dignity. Harm relating to an individual's loss of privacy and dignitary harm,

especially with information as sensitive as this, has also long been recognized by courts and in the common law.

49. When an individual loses this privacy and such sensitive information is viewed by a third party without their knowledge or consent, this harm cannot be undone. Weiss' unlawful and immoral violation of the personal and intimate lives of thousands of young people shocks the conscience and causes humiliation and loss of dignity that cannot be easily undone. The University Defendants and Keffer's failure to safeguard this sensitive information has stripped Plaintiff and the Class Members of this essential control, exposing them to the potential for enduring emotional distress and the profound sense of vulnerability that accompanies the exposure of deeply private matters.

50. By stripping Plaintiff and the Class Members of their right to control this sensitive information about themselves, Defendants have done immense harm to Plaintiff and the Class Members' rights to privacy as well as their personal dignity and bodily sovereignty. This permanent loss of security and fundamental right to privacy and bodily autonomy is harm that no compensation can ever fully restore.

TOLLING

51. Plaintiff realleges and incorporate by reference all preceding allegations as though fully set forth herein.

52. The statutes of limitations applicable to Plaintiff's claims were tolled by Defendants' conduct and Plaintiff's and Class Members delayed discovery of their claims.

53. As alleged above, Plaintiff did not know, and could not have known, that Defendant Weiss would have surreptitiously obtained her personal photographs and information without her consent.

54. The Defendants' alleged unlawful conduct could not have been discovered until at least March 2025 when Weiss was arrested and publicly indicted in federal court for his illegal access of thousands of accounts, including obtaining private and personal information on thousands of athletes at the University of Michigan and up to another 100 universities.

55. Plaintiff could not have discovered, through the exercise of reasonable diligence, the full scope of Defendants' alleged unlawful conduct, as Weiss surreptitiously accessed her information and the other Defendants failed to stop him or otherwise make Plaintiff and the Class Members aware of this illegal activity.

56. All applicable statutes of limitations have been tolled by operation of the delayed discovery rule. Under the circumstances, Defendants were under a duty to disclose the nature and significance of the invasion of privacy but did not do so. Defendants are therefore estopped from relying on any statute of limitations.

CLASS ACTION ALLEGATIONS

57. Plaintiff brings this action on her own behalf and on behalf of all other persons similarly situated.

58. Specifically, Plaintiff proposes the following classes (collectively, the “Class”):

All individuals whose Private Information was accessed without authorization by Matthew Weiss.

This definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

59. The Class is comprised of, at minimum, tens of thousands of students and student athletes, both at the University of Michigan as well as numerous other universities across the country, who had information exposed as part of Weiss’ illegal access (the “Class Members”). The Class is so numerous that joinder of all members is impracticable and the disposition of their claims in a class action will benefit the parties and the Court.

60. There is a well-defined community of interest in the questions of law and fact involved affecting the parties to be represented in that the Class was exposed to the same common harm. The questions of law and fact common to the Class predominate over questions which may affect individual Class members. Common questions of law and fact include, but are not limited to, the following:

- a. Whether Defendant Weiss surreptitiously entered and took Private Information from Plaintiff and Class Members;
- b. What information Defendant Weiss obtained from Plaintiff and the Class Members without their knowledge or consent;
- c. The method, or methods, by which Defendant Weiss obtained this Private Information;
- d. Whether the University Defendants' or Keffer's failure to implement effective security measures to protect Plaintiff's and the Class's Private Information was negligent;
- e. Whether the University Defendants were negligent in hiring, retaining, or supervising Defendant Weiss;
- f. Whether Defendant Keffer represented to Plaintiff and the Class that it would protect Plaintiff's and the Class Members' Private Information;
- g. Whether the Defendants owed a duty to Plaintiff the Class to exercise due care in collecting, storing, and safeguarding their Private Information;
- h. Whether the Defendants breached a duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

- i. Whether the Defendants' conduct caused or resulted in damages to Plaintiff and the Class;
- j. Whether Defendants failed to notify the public of the unlawful access in a timely and adequate manner;
- k. Whether Defendant Keffer or the University Defendants knew or should have known that their systems, including but not limited to training protocols and policies, left it vulnerable to unauthorized access;
- l. Whether Defendant Keffer or the University Defendants adequately addressed the vulnerabilities that allowed for Weiss' unauthorized access; and
- m. Whether, as a result of the Defendants' conduct, Plaintiff and the Class are entitled to damages and relief.

61. Plaintiff's claims are typical of the claims of the proposed Class, as Plaintiff and Class Members were harmed by the Defendants' uniform unlawful conduct.

62. Plaintiff will fairly and adequately represent and protect the interests of the proposed Class. Plaintiff has retained competent and experienced counsel in class action litigation and other complex litigation.

63. The Class is identifiable and readily ascertainable. Notice can be provided to such purchasers using techniques and a form of notice similar to those customarily used in class actions, and by internet publication, radio, newspapers, and magazines.

64. A class action is superior to other available methods for fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for proposed members of the Class to prosecute their claims individually.

65. The litigation and resolution of the Class's claims are manageable. Individual litigation of the legal and factual issues raised by the Defendants' conduct would increase delay and expense to all parties and the court system. The class action device presents far fewer management difficulties and provides the benefits of a single, uniform adjudication, economies of scale, and comprehensive supervision by a single court.

66. The Defendants have acted on grounds generally applicable to the entire Class, thereby making final injunctive relief and/or corresponding declaratory relief appropriate with respect to the Class as a whole. The prosecution of separate actions by individual Class Members would create the risk of inconsistent or varying adjudications with respect to individual member of the Class that would establish incompatible standards of conduct for the Defendants.

67. Absent a class action, Defendants will likely retain the benefits of their wrongdoing. Absent a representative action, Class Members will continue to suffer losses.

COUNT ONE

INVASION OF PRIVACY

(Against all Defendants and on Behalf of Plaintiff and the Class)

68. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

69. Plaintiff and the Class Members had a reasonable and legitimate expectation of privacy in their Private Information that the Defendants failed to adequately protect against compromise from unauthorized third parties.

70. The Defendants owed a duty to Plaintiff and Class Members to keep their Private Information confidential.

71. Defendant Keffer and the University Defendants failed to protect, and allowed the Private Information of Plaintiff and Class Members to be exfiltrated and stolen by Defendant Weiss.

72. Defendant Weiss additionally invaded the Privacy of Plaintiff and the Class Members by secretly obtaining their Private Information as well as photos, communications, and other information for his own personal and illicit use without the knowledge or consent of Plaintiff or the Class Members.

73. By failing to keep Plaintiff's and Class Members' Private Information safe, knowingly utilizing unsecure systems and practices, Defendants unlawfully invaded Plaintiff's and Class Members' privacy by, among others, (i) intruding into Plaintiff's and Class Members' private affairs in a manner that would be highly offensive to a reasonable person; (ii) failing to adequately secure their Private Information from disclosure to unauthorized persons and/or third parties; and (iii) enabling the disclosure of Plaintiff's and Class Members' Private Information without consent.

74. Defendants knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's and Class Members' position would consider their actions highly offensive.

75. The University Defendants and Keffer knew, or acted with reckless disregard of the fact that, organizations handling PII or PHI are highly vulnerable to cyberattacks and that employing inadequate security and training practices would render them especially vulnerable to data breaches.

76. As a proximate result of such unauthorized disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted, thereby causing Plaintiff and the Class Members undue harm.

77. The University Defendants are vicariously liable for Defendant Weiss' actions taken in his role as an employee of the University.

78. Plaintiff seeks injunctive relief on behalf of the Class, restitution, as well as any and all other relief that may be available at law or equity. Unless and until enjoined, and restrained by order of this Court, the Defendants' wrongful conduct will continue to cause irreparable injury to Plaintiff and Class Members as other individuals could access Plaintiff's and Class Members highly sensitive communications, messages, photographs, as well as health related information. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the class.

COUNT TWO

INTRUSION UPON SECLUSION

(Against All Defendants on Behalf of Plaintiff and the Class)

79. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

80. Plaintiff's and Class Members' Private Information is and always has been private and confidential.

81. Dissemination of Plaintiff's and Class Members' Private Information is not of a legitimate public concern; publication to third parties of their Private

Information would be, is and will continue to be, offensive to Plaintiff, Class Members, and other reasonable people.

82. By failing to keep Plaintiff's and Class Members' Private Information secure, and disclosing Private Information to unauthorized parties for unauthorized use, Defendant Keffer and the University Defendants unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion.

83. Defendant Keffer and the University Defendants' wrongful actions and/or inaction constituted, and continue to constitute, an invasion of Plaintiff's and Class Members' privacy by publicly disclosing their Private Information when they allowed Defendant Weiss to exfiltrate large amounts of Private Information regarding student athletes at the University as well as other institutions.

84. Defendant Weiss also directly invaded the privacy of Plaintiff and the Class Members when he exfiltrated large amounts of data from the computer systems of Keffer and the University Defendants as well as hacking into the personal accounts of thousands of students, student athletes, and alumni.

85. Defendant Weiss' intrusions were substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

86. Plaintiff and the Class Members were, and continue to be, damaged as a direct and proximate result of the Defendants' invasion of their privacy by publicly

disclosing their Private Information, for which they suffered loss and are entitled to compensation.

87. The University Defendants are vicariously liable for Defendant Weiss' actions taken in his role as an employee of the University.

88. As a direct and proximate result of the Defendants' violations, Plaintiff and the Class have suffered and continue to suffer injury.

COUNT THREE

NEGLIGENCE

(Against Keffer and the University Defendants and on Behalf of Plaintiff and the Class)

89. Plaintiff, individually and on behalf of the Class, herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

90. The University Defendants and Keffer owed a duty to act with due and reasonable care towards the public and in particular the students of the University as well as other individuals whose information was within Keffer's computer system.

91. The University Defendants and Keffer were aware that its students and especially student athletes could be in danger from staff, especially as the University

of Michigan had settled a case involving a physician that had abused hundreds of student athletes over a period of decades.²⁰

92. Defendant Keffer, however, did not ensure that its communication system was secure and could adequately protect the users of its service, including the student athletes.

93. The University Defendants also failed to implement policies and procedures to ensure that their staff, especially coaches and other athletic trainers who by nature of their role have a great deal of power over students, were adequately monitored and supervised to ensure that they did not mistreat students including by hacking into their accounts or otherwise obtaining information secretly.

94. At all times relevant, the University Defendants were well aware of the dangers its athletic employees could pose and the vulnerable place its student athletes were in, but failed to do what was necessary in order to ensure they were protected. The University Defendants were aware that their student athletes depend on them to provide a safe environment, but they failed to do so by neglecting their responsibility and allowing Defendant Weiss to hack into and obtain enormous amounts of private information on them without their knowledge.

²⁰ Ivan Pereira, *University of Michigan reaches \$490M settlement with sex abuse survivors*, ABC NEWS (Jan. 19, 2022), <https://abcnews.go.com/US/university-michigan-reaches-490m-settlement-sex-abuse-survivors/story?id=82353991>.

95. Defendant Keffer also knew the sensitivity of the information kept on its system but failed to ensure that it was secure.

96. For the above reasons and others, the University Defendants and Keffer breached the duty of reasonable care to Plaintiff and the Class Members.

97. As a legal and direct result of the University Defendants and Keffer's actions and omissions, Plaintiff and the Class Members had their personal information targeted, stolen, and viewed without their knowledge or permission, including highly sensitive information such as intimate photos, private communications, and other information.

98. As a direct and proximate result of the University Defendants and Keffer's general negligence, Plaintiff suffered economic and non-economic damages.

99. Plaintiff, individually, on behalf of the Class members, seeks all monetary and non-monetary relief allowed by law, including actual damages, statutory damages, punitive damages, preliminary and other equitable or declaratory relief, and attorneys' fees and costs.

///

///

///

COUNT FOUR

NEGLIGENT HIRING, RETENTION, AND SUPERVISION

(Against the University Defendants on Behalf of Plaintiff and the Class)

100. Plaintiff, Individually and on behalf of the Class, herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

101. the University Defendants engaged and retained or otherwise employed Defendant Weiss, who hacked into student athletes accounts and stole and viewed information between approximately 2015-2023.

102. The University Defendants did not adequately interview, vet, or screen Weiss when hiring him. The University Defendants failed to use reasonable care to discover his lack of fitness to work at the University due to his frequent and extensive invasion of students' privacy.

103. Despite failing to reasonably endeavor to investigate Weiss, the University Defendants hired him and gave him access to student athletes and their information.

104. The University Defendants knew or should have known of the risks.

105. The University Defendants failed to employ measures to adequately supervise Weiss.

106. The University Defendants were negligent in failing to discover Defendant Weiss' actions on its computer systems for the 8 years he did so.

107. Because of the University Defendants’ failure to adequately screen and supervise Defendant Weiss, Plaintiff and the Class Members had their privacy invaded, personal photos and communications stolen, and otherwise subject to an invasion of privacy and violation of their fundamental rights.

108. The University Defendants’ negligence in hiring, retaining, and or supervising Weiss, caused Plaintiff and the Class Members to have their privacy invaded and personal photos and communications viewed without their knowledge or consent, which humiliated, degraded, violated, and robbed Plaintiff and the Class Members of their dignity and personal safety.

109. As a direct and proximate result of the University Defendants’ negligent supervision, hiring, and retention Weiss, Plaintiff suffered economic and non-economic damages.

110. Plaintiff, individually, on behalf of the Class members, seeks all monetary and non-monetary relief allowed by law, including actual damages, statutory damages, punitive damages, preliminary and other equitable or declaratory relief, and attorneys’ fees and costs.

///

///

///

///

COUNT FIVE

STORED COMMUNICATIONS ACT

(Against all Defendants and on Behalf of Plaintiff and the Class)

111. Plaintiff, Individually and on behalf of the Class, herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

112. A violation of the Stored Communications Act (“SCA”) occurs when anyone “intentionally accesses without authorization a facility through which an electronic communication service is provided.” 18 U.S.C. § 2701(a).

113. 18 U.S.C. § 2707(a) provides a private right of action to anyone “aggrieved by any violation” engaged in with a “knowing or intentional state of mind.”

114. Keffer’s computer system that Weiss used, while employed by and acting for the University Defendants, is a “facility” as defined by the SCA, as it stores the personal information of Plaintiff and the Class Members as well as communications from them.

115. Defendant Keffer allowed Defendant Weiss to access electronic communications, as well as private and confidential emails, messages, photos, and other sensitive information – all stored on cloud servers, without authorization. Weiss, using Defendants’ computer systems (due to their vulnerability) gained access to the student accounts. Defendants failed to detect his “inside hacking” and

allowed Weis surreptitious entry and exfiltration of Plaintiff's and the Class Members' photos, confidential communications, and personal information.

116. Plaintiff and Class members did not have knowledge of, authorize, or consent to Defendant Weiss' accessibility to Plaintiff's and Class members' Private Information stored in Keffer's computer system.

117. Defendant Weiss' access of Plaintiff's and Class members' personally identifiable information and constitutes "unauthorized access" within the meaning of 18 U.S.C. § 2701(a) because Plaintiff and Class members had no reasonable expectation their Private Information, emails, messages, and intimate photos would be shared with anyone – including Defendants and Weiss.

118. Defendant Weiss intentionally exceeded its authorization to access the Plaintiff's and Class members' Private Information and other information and communications through Keffer's computer system in violation of 18 U.S.C. § 2701(a)(2).

119. Keffer failed to ensure its computer system was secure or restrict usage of it to prevent individuals such as Defendant Weiss from surreptitiously obtaining Plaintiff's and the Class Members' Private Information.

120. Due to the Defendants' failures to comply with the law, Plaintiff and the Class Members suffered injury.

121. The University Defendants are vicariously liable for Defendant Weiss' actions taken in his role as an employee of the University.

122. Plaintiff, individually, on behalf of the Class members, seeks all monetary and non-monetary relief allowed by law, including actual damages, statutory damages, punitive damages, preliminary and other equitable or declaratory relief, and attorneys' fees and costs.

COUNT SIX

VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C. § 1983- INVASION OF PRIVACY

(Against the University Defendants on Behalf of Plaintiff and the Class)

123. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

124. The University Defendants at all times relevant to this action were acting under color of state law.

125. Plaintiff and the Class Members had a constitutional right to privacy and to not be deprived of life, liberty, or property without due process as guaranteed under the Fourteenth Amendment of the U.S. Constitution.

126. The University Defendants hired Weiss and put him in a position wherein he was able to invade the privacy of Plaintiff and the Class Members.

127. Plaintiff and the Class Members were foreseeable victims of Defendant Weiss, but the University Defendants failed to ensure their safety.

128. Due to the University Defendants' failure to ensure the safety, security, and privacy of Plaintiff and the Class Members, their Private Information was obtained by Weiss and potentially exposed to additionally and currently unknown third parties.

129. The University Defendants acted in a willful disregard for the rights and safety of Plaintiff and the Class Members and allowed Weiss in a position wherein he could, and did, harm Plaintiff and the Class Members through the invasion of their privacy.

130. Due to the Defendants' failures to comply with the law, Plaintiff and the Class Members suffered injury.

131. The University Defendants are vicariously liable for Defendant Weiss' actions taken in his role as an employee of the University.

132. Plaintiff, individually, on behalf of the Class members, seeks all monetary and non-monetary relief allowed by law, including actual damages, statutory damages, punitive damages, preliminary and other equitable or declaratory relief, and attorneys' fees and costs.

COUNT SEVEN

VIOLATIONS OF MICH. COMP. LAWS § 600.2919

(Against Weiss and the University Defendants and on Behalf of Plaintiff and the Class)

133. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

134. Mich. Comp. Laws § 600.2919a provides that a person “damaged as a result of...[a]nother person’s stealing or embezzling property or converting property to the other person’s own use...” may recover three times the amount of actual damages, plus reasonable attorney’s fees and costs.

135. Plaintiff and the Class Member were the victims of Defendant Weiss’ theft of their personal information and suffered damages as a result.

136. Defendant Weiss additionally converted Plaintiff and the Class Members’ Private Information to his own use when he secretly stole it and used it for his own purposes without the knowledge or consent of Plaintiff or the Class Members.

137. The University Defendants are vicariously liable for Defendant Weiss’ actions taken in his role as an employee of the University.

138. Plaintiff, individually, on behalf of the Class members, seeks all monetary and non-monetary relief allowed by law, including actual damages,

statutory damages, punitive damages, preliminary and other equitable or declaratory relief, and attorneys' fees and costs.

COUNT EIGHT

MICHIGAN IDENTITY THEFT PROTECTION ACT

(Mich. Comp. Laws § 445.72, *et. seq.*)

(Against Defendants and on Behalf of Plaintiff and the Class)

139. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

140. As entities that collects, disseminates, and otherwise deals with nonpublic Private Information, The University Defendants and Keffer are each a “person or agency that owns or licenses data” of residents of the State of Michigan under Mich. Comp. Laws Ann. § 445.72(1)(a).

141. Plaintiff and the Class Members' Private Information includes “personal information” as covered under Mich. Comp. Laws Ann. § 445.63(r). 3750.

142. The University Defendants and Keffer were required to notify Plaintiff and the Class Members of a breach of their data security system in the most expedient time possible and without unreasonable delay if a Michigan resident's unencrypted and unredacted personal information is accessed or acquired by an unauthorized person pursuant to Mich. Comp. Laws Ann. §§ 445.72(1)(a), (4).

143. Upon information and belief, Plaintiff and the Class Members' unencrypted and unredacted personal information was accessed or compromised by Defendant Weiss without their authorization.

144. Defendant Weiss' illicit theft and interception of the Private Information described herein constituted a "breach of the security of a database" of Keffer.

145. Defendant Weiss violated the Identity Theft Protect Act by obtaining Plaintiff and the Class Members' Private Information in violation with the intent to violate the law, in violation of § 445.65.

146. Because the University Defendants and Keffer knew or should have known that Plaintiff and the Class Members' Private Information was acquired by Weiss without authorization, they had an obligation to disclose the breach in a timely and accurate fashion.

147. As alleged above, the University Defendants and Keffer unreasonably delayed informing Plaintiff and the Class Members about Weiss' unauthorized access, affecting their Private Information, after they knew that the unauthorized access had occurred.

148. By failing to disclose the unauthorized access in the most expedient time possible and without unreasonable delay, the University Defendants and Keffer violated Mich. Comp. Laws Ann. §§ 445.72(1)(a)(4).

149. As a result of the University Defendants and Keffer violation of Mich. Comp. Laws Ann. §§ 445.72(1)(a)(4), Plaintiff and the Class Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures.

150. As a result of the University Defendants and Keffer violation of Mich. Comp. Laws Ann. §§ 445.72(1)(a)(4), Plaintiff and the Class Members suffered incrementally increased damages separate and distinct from those simply caused by the unauthorized access itself.

151. The University Defendants are vicariously liable for Defendant Weiss' actions taken in his role as an employee of the University.

152. While the Identity Theft Protection Act does not have a specific private right of action, the statute makes clear that it does not affect "the availability of any civil remedy for a violation of state or federal law." Mich. Comp. Laws Ann. § 445.72(15)

153. Plaintiff, individually, on behalf of the Class members, seek any and all available relief under Michigan law pursuant to Mich. Comp. Laws Ann. § 445.72(15).

COUNT NINE

DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF

(Against all Defendants and on Behalf of Plaintiff and the Class)

154. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

155. The Declaratory Judgment Act, 28 U.S.C. § 2201, et seq., authorizes this Court to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief.

156. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the statutes described in this Complaint.

157. The University Defendants and Keffer owe a duty of care to Plaintiff and Class Members which require it to adequately secure their Private Information when they chose to accept and store Plaintiff's and Class Members' Private Information.

158. The University Defendants and Keffer still possess Plaintiff's and Class Members' Private Information.

159. The University Defendants and Keffer have not made clear what specific and verifiable steps they have taken to prevent a similar breach from occurring again.

160. Plaintiff and Class Members are at risk of harm due to the exposure of their Private Information and the University Defendants and Keffer failures to address the security failings that lead to such exposure.

161. An actual controversy has arisen regarding the University Defendants and Keffer's present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class Members' Private Information and whether the University Defendants and Keffer are currently maintaining data security measures adequate to protect Plaintiff and the Class from further actions compromising their Private Information.

162. Plaintiff and the Class, therefore, seek a declaration that (1) each of the University Defendants and Keffer's existing security measures do not comply with its obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect students' Private Information, and (2) to comply with its duties of care, the University Defendants and Keffer must implement and maintain reasonable security measures, including, but not limited to:

- a. Prohibiting the University Defendants and Keffer from engaging in the wrongful acts stated herein;
- b. Requiring the University Defendants and Keffer to implement adequate security protocols and practices to protect their

students' Private Information consistent with the industry standards, applicable regulations, and federal, state, and/or local laws;

- c. Mandating the proper notice be sent to all affected students and alumni, and posted publicly;
- d. Requiring the University Defendants and Keffer to protect all data collected;
- e. Requiring the University Defendants and Keffer to delete, destroy, and purge the Private Information of Plaintiff and Class Members unless they can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
- f. Requiring the University Defendants and Keffer to implement and maintain a comprehensive security program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' Private Information;
- g. Requiring the University Defendants and Keffer to engage independent third-party security auditors and conduct internal security audit and testing, including simulated attacks,

penetration tests, and audits on the University Defendants and Keffer's systems on a periodic basis;

- h. Requiring the University Defendants and Keffer to engage independent third-party security auditors and/or internal personnel to run automated security monitoring;
- i. Requiring the University Defendants and Keffer to enact policies and procedures sufficient to ensure that only individuals with the appropriate training and access may be allowed to access the Private Information data and that the viewing of the data is monitored, logged, reported and regularly analyzed to ensure it is not misused;
- j. Cooperating with Plaintiff and the Class Members in analyzing what data was specifically viewed and whether that Private Information was shared beyond Defendant Weiss; and
- k. Requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

163. The Court can, and should, issue corresponding prospective injunctive relief requiring the University Defendants and Keffer to employ adequate security

protocols consistent with the law and industry standards to protect Plaintiff's and Class Members' Private Information.

164. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of the University Defendants and Keffer's systems or networks.

165. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to the University Defendants and Keffer if an injunction is issued. The cost to the University Defendants and Keffer of complying with an injunction by employing reasonable prospective data security measures is minimal given they have preexisting legal obligations to employ these measures.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, requests judgment and relief on all causes of action as follows:

- A. That the Court determines that this Action may be maintained as a Class Action, that Plaintiff be named as Class Representative of the Class, that the undersigned be named as Class Counsel of the Class, and that notice of this Action be given to Class Members;

- B. That the Court enter an order declaring that the Defendants' actions, as set forth in this Complaint, violate the laws set forth above;
- C. That the Court enter an order providing declaratory and injunctive relief including specific steps, as outlined above, requiring Defendants to utilize appropriate methods and policies as necessary to remediate the harm suffered by Plaintiff and the Class members as well as to prevent future harm and properly secure its data, and to provide sufficient and timely notice for all Class Members;
- D. That the Court award Plaintiff and the Class damages (both actual damages for economic and non-economic harm and statutory damages) in an amount to be determined at trial;
- E. That the Court issue appropriate equitable and any other relief (including monetary damages, restitution, and/or disgorgement) against Defendant to which Plaintiff and the Class are entitled;
- F. That the Court award Plaintiff and the Class pre- and post-judgment interest (including pursuant to statutory rates of interest set under State law);

- G. That the Court award Plaintiff and the Class their reasonable attorneys' fees and costs of suit;
- H. That the Court award treble and/or punitive damages insofar as they are allowed by applicable laws; and
- I. That the Court award any and all other such relief as the Court may deem just and proper under the circumstances.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff respectfully demands a trial by jury for all claims.

DATED: March 27, 2025

Respectfully submitted,
CLARKSON LAW FIRM, P.C.

By: /s/ Ryan J. Clarkson
Ryan J. Clarkson, (P68616)
rclarkson@clarksonlawfirm.com
Yana Hart*
yhart@clarksonlawfirm.com
Bryan P. Thompson*
bthompson@clarksonlawfirm.com
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
Fax: (213) 788-4070

**Pro Hac Vice Forthcoming*

*Counsel for Plaintiff and
the Putative Class*

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

JANE ROE CLF 001, individually and on behalf of all others similarly situated,

(b) County of Residence of First Listed Plaintiff Washtenaw
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

Ryan J. Clarkson, Esq.
Clarkson Law Firm, P.C.
22525 Pacific Coast Highway, Malibu, CA 90265, Tel: (213) 788-4050

DEFENDANTS

MATTHEW WEISS; THE REGENTS OF THE UNIVERSITY OF MICHIGAN; THE UNIVERSITY OF MICHIGAN; KEFFER DEVELOPMENT SERVICES, LLC

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff ☐ 3 Federal Question (U.S. Government Not a Party)
- ☐ 2 U.S. Government Defendant ☒ 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- | | PTF | DEF | | PTF | DEF |
|---|---------------------------------------|----------------------------|---|----------------------------|---------------------------------------|
| Citizen of This State | <input checked="" type="checkbox"/> 1 | <input type="checkbox"/> 1 | Incorporated or Principal Place of Business In This State | <input type="checkbox"/> 4 | <input checked="" type="checkbox"/> 4 |
| Citizen of Another State | <input type="checkbox"/> 2 | <input type="checkbox"/> 2 | Incorporated and Principal Place of Business In Another State | <input type="checkbox"/> 5 | <input type="checkbox"/> 5 |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3 | <input type="checkbox"/> 3 | Foreign Nation | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 |

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Click here for: [Nature of Suit Code Descriptions.](#)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES	
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice	PERSONAL INJURY <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act IMMIGRATION <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 PROPERTY RIGHTS <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 835 Patent - Abbreviated New Drug Application <input type="checkbox"/> 840 Trademark <input type="checkbox"/> 880 Defend Trade Secrets Act of 2016 SOCIAL SECURITY <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit (15 USC 1681 or 1692) <input type="checkbox"/> 485 Telephone Consumer Protection Act <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
REAL PROPERTY <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	CIVIL RIGHTS <input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education	PRISONER PETITIONS Habeas Corpus: <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty Other: <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN (Place an "X" in One Box Only)

- ☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District (specify) ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
28 U.S.C 1332(d)(2)
Brief description of cause:
Invasion of Privacy

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P. DEMAND \$ 100,000,000.00 CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE DOCKET NUMBER

DATE

March 27, 2025

SIGNATURE OF ATTORNEY OF RECORD

/s/ Ryan J. Clarkson

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

1. Is this a case that has been previously dismissed?

☐ Yes
☒ No

If yes, give the following information:

Court: _____

Case No.: _____

Judge: _____

2. Other than stated above, are there any pending or previously discontinued or dismissed companion cases in this or any other court, including state court? (Companion cases are matters in which it appears substantially similar evidence will be offered or the same or related parties are present and the cases arise out of the same transaction or occurrence.)

☒ Yes
☐ No

If yes, give the following information:

Court: E.D. Michigan - Southern Division

Case No.: 2:25-cv-10806; 2:25-cv-10855

Judge: Mark A. Goldsmith; Linda V. Parker

Notes :

[Query](#) [Reports](#) [Utilities](#) [Help](#) [Log Out](#)

WEISMAN

United States District Court
Northern District of Illinois - CM/ECF NextGen 1.8 (rev. 1.8.3) (Chicago)
CIVIL DOCKET FOR CASE #: 1:25-cv-04233

DOE v. Weiss et al
Assigned to: Honorable Matthew F. Kennelly
Cause: 28:1331 Federal Question

Date Filed: 04/17/2025
Jury Demand: Plaintiff
Nature of Suit: 890 Other Statutory Actions
Jurisdiction: Federal Question

Plaintiff**JANE DOE**

represented by **Jason J Thompson**
Sommers Schwartz, Pc
1 Towne Square, Suite 1700
Southfield, MI 48076
(248) 355-0300
Fax: Not a member
Email: jthompson@sommerspc.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Jacob Mayer Podell
Wallace Miller
150 N Wacker Dr
Chicago, IL 60606
(312) 261-6193
Fax: Not a member
Email: jpodell@wallacemiller.com
ATTORNEY TO BE NOTICED

Matthew G Curtis , Male
Sommers Schwartz, P.C.
One Towne Square
17th Floor
Southfield
Southfield, MI 48076
248-746-4038
Fax: 248-936-2124
Email: mcurtis@sommerspc.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

Megan A. Bonanni
Pitt McGehee Palmer Bonanni & Rivers, PC
117 W. Fourth Street, Suite 200
Suite 200
Royal Oak, MI 48067
248-398-9800

Fax: 248-268-7996
Email: mbonanni@pittlawpc.com
ATTORNEY TO BE NOTICED

Richard Groffsky
Sommers Schwartz, P.C.
One Towne Square, 17th Floor
Southfield, MI 48076
(248) 355-0300
Fax: Pro Hac Vice
Email: rgroffsky@sommerspc.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

Edward A. Wallace
Wallace Miller
150 N Wacker
Ste 1100
Chicago, IL 60606
312-261-6193
Fax: 312-275-8174
Email: eaw@wallacemiller.com
ATTORNEY TO BE NOTICED

V.

Defendant

Matthew Weiss

Defendant

Loyola University Chicago

represented by **Mary S DiRago**
Troutman Pepper Locke LLP
111 South Wacker Drive
Suite 4100
Chicago, IL 60606
312-759-1926
Fax: 312-759-1939
Email: molly.dirago@troutman.com
ATTORNEY TO BE NOTICED

Defendant

Keffer Development Services, LLC

Date Filed	#	Docket Text
04/17/2025	1	COMPLAINT filed by JANE DOE; Jury Demand. Filing fee \$ 405, receipt number AILNDC-23365545. (Attachments: # 1 Exhibit A - DOJ Letter REDACTED)(Wallace, Edward) (Entered: 04/17/2025)
04/17/2025	2	CIVIL Cover Sheet (Wallace, Edward) (Entered: 04/17/2025)
04/17/2025	3	MOTION by Plaintiff JANE DOE for leave to file <i>Document Under Seal</i>

		(Wallace, Edward) (Entered: 04/17/2025)
04/17/2025	4	SEALED DOCUMENT by Plaintiff JANE DOE <i>Exhibit A to Complaint</i> (Wallace, Edward) (Entered: 04/17/2025)
04/17/2025	5	ATTORNEY Appearance for Plaintiff JANE DOE by Edward A. Wallace (Wallace, Edward) (Entered: 04/17/2025)
04/18/2025		CASE ASSIGNED to the Honorable Matthew F. Kennelly. Designated as Magistrate Judge the Honorable M. David Weisman. Case assignment: Random assignment. (Civil Category 1). (qrtr,) (Entered: 04/18/2025)
04/18/2025		CLERK'S NOTICE: Pursuant to Local Rule 73.1(b), a United States Magistrate Judge of this court is available to conduct all proceedings in this civil action. If all parties consent to have the currently assigned United States Magistrate Judge conduct all proceedings in this case, including trial, the entry of final judgment, and all post-trial proceedings, all parties must sign their names on the attached Consent To form. This consent form is eligible for filing only if executed by all parties. The parties can also express their consent to jurisdiction by a magistrate judge in any joint filing, including the Joint Initial Status Report or proposed Case Management Order. (qrtr,) (Entered: 04/18/2025)
04/22/2025	10	SUMMONS Issued (Court Participant) as to Defendants Keffer Development Services, LLC, Loyola University Chicago (Attachments: # 1 Summons Keffer)(txd,) (Entered: 04/22/2025)
04/23/2025	11	NOTICE by All Plaintiffs <i>of Filing Motion for Staus Conference</i> (Thompson, Jason) (Entered: 04/23/2025)
04/28/2025	12	ATTORNEY Appearance for Plaintiff JANE DOE by Jason J Thompson (Thompson, Jason) (Entered: 04/28/2025)
04/30/2025	13	MOTION for Leave to Appear Pro Hac Vice on behalf of JANE DOE by Megan A. Bonanni; Filing fee \$ 150, receipt number AILNDC-23419852. (Bonanni, Megan) (Entered: 04/30/2025)
05/01/2025	14	MINUTE entry before the Honorable Matthew F. Kennelly: Motion by Megan Bonanni to appear pro hac vice is granted 13 . (mk) (Entered: 05/01/2025)
05/01/2025	15	MINUTE entry before the Honorable Matthew F. Kennelly: This case is set for a telephonic status hearing on 5/6/2025 at 8:55 AM (Central Time), using call-in number 650-479-3207, access code 2305-915-8729. Plaintiff's counsel is directed to advise defendants' counsel in the related E.D. Mich. cases regarding the date and time and call-in information for the status hearing. (mk) (Entered: 05/01/2025)
05/05/2025	16	WAIVER OF SERVICE returned executed by JANE DOE. Keffer Development Services, LLC waiver sent on 4/28/2025, answer due 6/27/2025. (Wallace, Edward) (Entered: 05/05/2025)
05/06/2025	17	MINUTE entry before the Honorable Matthew F. Kennelly: Telephonic status hearing held on 5/6/2025. Plaintiff's motion to file under seal 3 is granted. The case will set a further status hearing at a later date. Mailed notice. (mma,) (Entered: 05/06/2025)
05/08/2025	18	ATTORNEY Appearance for Plaintiff JANE DOE by Megan A. Bonanni (Bonanni, Megan) (Entered: 05/08/2025)
05/08/2025	19	SUMMONS Returned Executed by JANE DOE as to Loyola University Chicago on 5/5/2025, answer due 5/26/2025. (Wallace, Edward) (Entered: 05/08/2025)

05/09/2025	20	MOTION for Leave to Appear Pro Hac Vice on behalf of JANE DOE by Lisa Marie Esser; Filing fee \$ 150, receipt number AILNDC-23462916. (Esser, Lisa) (Entered: 05/09/2025)
05/10/2025	21	MINUTE entry before the Honorable Matthew F. Kennelly: Motion by Lisa M. Esser to appear pro hac vice 20 is granted. (mk) (Entered: 05/10/2025)
05/13/2025	23	SUMMONS Issued (Court Participant) as to Defendant Matthew Weiss (cvk,) (Entered: 05/13/2025)
05/13/2025	24	ATTORNEY Appearance for Plaintiff JANE DOE by Jacob Mayer Podell (Podell, Jacob) (Entered: 05/13/2025)
05/13/2025	25	PAYMENT by JANE DOE of Pro Hac Fee \$ 150, receipt number AILNDC-23478444. (Groffsky, Richard) (Entered: 05/13/2025)
05/13/2025	26	<i>Pro Hac Fee \$ 150,see receipt number AILNDC-23478444</i> MOTION by Plaintiff JANE DOE for leave to appear as Pro Hac Vice <i>Pro Hac Fee \$ 150,see receipt number AILNDC-23478444</i> (Groffsky, Richard) (Entered: 05/13/2025)
05/13/2025	27	MOTION for Leave to Appear Pro Hac Vice on behalf of JANE DOE by Matthew G Curtis, Male; Filing fee \$ 150, receipt number AILNDC-23478592. (Curtis, Matthew) (Entered: 05/13/2025)
05/14/2025	28	MINUTE entry before the Honorable Matthew F. Kennelly: Motions by Richard Groffsky 26 and Matthew Curtis 27 to appear pro hac vice are granted. (mk) (Entered: 05/14/2025)
05/29/2025	29	MINUTE entry before the Honorable Matthew F. Kennelly: By no later than 6/6/2025, the parties (or, if no defendant has yet appeared, the plaintiff(s)) are to file a joint status report that includes the following information: (1) the status of service of process upon each defendant; (2) a description of each party's claims and defenses; (3) details regarding any discussions concerning settlement, whether before or after the filing of the lawsuit; (4) a proposed discovery and pretrial schedule; and (5) any other matters that any party wishes to bring to the Court's attention. The case is set for a case management conference under Federal Rule of Civil Procedure 16 on 6/13/2025 at 9:00 a.m. The case management conference will be conducted by telephone, using the following call-in number: 650-479-3207, access code 2305-915-8729. Plaintiff's counsel is directed to provide a copy of this order to any defendant that has not yet appeared by counsel via regular mail at the address at which the defendant has been or is to be served with process. (mk) (Entered: 05/29/2025)
05/30/2025	30	ATTORNEY Appearance for Defendant Loyola University Chicago by Mary S DiRago (DiRago, Mary) (Entered: 05/30/2025)
05/30/2025	31	MOTION by Defendant Loyola University Chicago for extension of time <i>Agreed Motion to Extend Time for Defendant Loyola University Chicago to Respond to Class Action Complaint</i> (DiRago, Mary) (Entered: 05/30/2025)
05/31/2025	32	MINUTE entry before the Honorable Matthew F. Kennelly: By no later than 6/19/2025, the parties (or, if no defendant has yet appeared, the plaintiff(s)) are to file a joint status report that includes the following information: (1) the status of service of process upon each defendant; (2) a description of each party's claims and defenses; (3) details regarding

		any discussions concerning settlement, whether before or after the filing of the lawsuit; (4) a proposed discovery and pretrial schedule; and (5) any other matters that any party wishes to bring to the Court's attention. The case is set for a case management conference under Federal Rule of Civil Procedure 16 on 6/26/2025 at 8:50 a.m. The case management conference will be conducted by telephone, using the following call-in number: 650-479-3207, access code 2305-915-8729. Plaintiff's counsel is directed to provide a copy of this order to any defendant that has not yet appeared by counsel via regular mail at the address at which the defendant has been or is to be served with process. In addition, defendant Loyola's unopposed motion for extension of time 31 is granted; response to complaint is to be filed by 6/26/2025. (mk) (Entered: 05/31/2025)
05/31/2025	33	MINUTE entry before the Honorable Matthew F. Kennelly: Telephonic status hearing set for 6/26/2025 at 8:50 AM. (mk) (Entered: 05/31/2025)
05/31/2025	34	MINUTE entry before the Honorable Matthew F. Kennelly: Minute entries 32 and 33, dated 5/31/2025, are vacated to the extent they ordered the filing of a stats report on 6/19/2025 and set a status hearing on 6/26/2025. The dates for the initial status report and status hearing had already been set by prior order of court. (mk) (Entered: 05/31/2025)

PACER Service Center			
Transaction Receipt			
06/05/2025 15:11:50			
PACER Login:	ThomaKingtking	Client Code:	
Description:	Docket Report	Search Criteria:	1:25-cv-04233
Billable Pages:	4	Cost:	0.40

**IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS**

JANE DOE 1, on behalf of herself and all
others similarly situated,

Plaintiff,

-against-

MATTHEW WEISS, LOYOLA UNIVERSITY
CHICAGO, AND KEFFER DEVELOPMENT
SERVICES, LLC,

Defendants.

Case No. 1:25-cv-04233

JURY TRIAL DEMANDED

PLAINTIFF'S CLASS ACTION COMPLAINT

Plaintiff JANE DOE 1, through her attorneys, Sommers Schwartz, P.C., Pitt McGehee Palmer Bonanni & Rivers, P.C., and Wallace Miller, for their Complaint against MATTHEW WEISS, LOYOLA UNIVERSITY CHICAGO, and KEFFER DEVELOPMENT SERVICES, LLC, states as follows:

I. INTRODUCTION

Students and alumni connected to Loyola University Chicago from 2015 to 2023—many of them student-athletes—have been subjected to a deeply troubling and unlawful breach of privacy, stemming from the actions of former University of Michigan and Baltimore Ravens football coach Matthew Weiss, whose gross and despicable violations of their privacy were facilitated by institutional negligence. This class action lawsuit, filed against Matthew Weiss, Loyola University Chicago, and Keffer Development Services, LLC, seeks justice for the unauthorized access and misuse of personal information—an abuse so severe that Loyola

University Chicago students and student-athletes are now receiving formal notification from the U.S. Department of Justice that their private information, including intimate photos and videos, have been exposed, including Plaintiff Jane Doe 1. This action is brought to hold the Defendants accountable for failing to protect their students from foreseeable harm.

II. PARTIES

1. Plaintiff Jane Doe 1 was a student athlete at Loyola University Chicago between 2014-2019 and was a member of the Volleyball Team.

2. Plaintiff Jane Doe 1 is domiciled in Florida, in the City of Jupiter.

3. On or about March 25, 2025, Plaintiff Jane Doe 1 received notice from the United States Department of Justice Victim Notification System that she was identified as a victim in the criminal case against University of Michigan's Coach Weiss: *United States v. Defendant(s) Matthew Weiss*.¹

4. Defendant Loyola University Chicago ("University") is a private university with its headquarters, domicile, and principal place of business in Chicago, Illinois.

5. Loyola University Chicago enrolls approximately 16,000 undergraduate and graduate students.

6. Loyola University Chicago is a member of the National Collegiate Athletic Association (NCAA), with over 300 student athletes competing in 16 intercollegiate sports at the Division 1 level.

7. Defendant Keffer Development Services, LLC ("Keffer") is a Pennsylvania limited liability company in Grove City, PA, that has continuously and systemically conducted business

¹ Jane Doe 1's DOJ Data Breach Notice is attached hereto as **Exhibit A**.

in Illinois by directly providing services to residents and entities within the State of Illinois, including its business contacts with Loyola University Chicago in Illinois, thereby availing itself of protections of the law of the State of Illinois.

8. Defendant Keffer is a technology and data vendor operating an electronic medical record and student athlete training system, which stored the personal identifying information (“PII”) and personal health information (“PHI”) of Plaintiff and Class Members across the country.

9. The wrongful conduct and legal violations committed by Defendant Keffer that are subsequently outlined in this Complaint occurred specifically with respect to the Plaintiff during the time of the incident alleged in this Complaint.

10. Matthew Weiss (“Weiss”) is an individual residing in the State of Michigan, who had contacts with the State of Illinois in that he conducted illegal activity in the State of Illinois, by hacking into the personal property of Plaintiff and putative Class Members of the State of Illinois during the applicable time period at issue in this Complaint and said activities from which this Complaint arises.

11. On March 20, 2025, Defendant Weiss was indicted on 24 counts of unauthorized access to computers and aggravated identity theft by the U.S. Attorney for the Eastern District of Michigan.

III. JURISDICTION AND VENUE

12. Jurisdiction is proper in this Court under 28 U.S.C. §§ 1331 and 1367 as this matter involves a claim under the Stored Communications Act, 18 U.S.C. § 2701(a) *et seq.*; the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; Title IX, 20 U.S.C. § 1681(A) *et seq.*; 42 U.S.C. § 1983; the Fourth Amendment of the U.S. Constitution; and the Fourteenth Amendment of the U.S.

Constitution, and this Court has supplemental jurisdiction of all additional causes of action alleged in this Complaint pursuant to 28 U.S.C. §1367(a).

13. This Court also has subject matter jurisdiction pursuant to 28 U.S.C. §1332(d) under the Class Action Fairness Act (“CAFA”) as a class action lawsuit in which the amount in controversy exceeds \$5,000,000.00, there are more than one-hundred putative Class Members, and the majority of the putative Class Members are citizens of a state different than the state of which Defendants are citizens.

14. The Court has personal jurisdiction over Defendants named in this action because Defendant University is located and created under the laws of the State of Illinois, and Defendant Weiss had minimum contacts with the State of Illinois as set forth above, thus purposefully availing himself of the privilege of conducting activities in the State of Illinois. Defendant Keffer conducts business at the State of Illinois and has availed itself of the protections of Illinois state law. The claims at issue in this case arise out of Defendants’ purposeful contacts with and business activities in the State of Illinois.

15. Venue is appropriate in this District Court under 28 U.S.C. §1391(b) since a substantial part of the events or omissions giving rise to these claims occurred within this District.

16. Plaintiff’s injuries are redressable by monetary compensation, and all alleged injuries of Plaintiff and Class Members can be traced to Defendants’ conduct.

IV. COMMON ALLEGATIONS

A. WEISS’S DATA BREACH AND CYBER SEXUAL ASSAULT OF THOUSANDS OF STUDENTS FOR NEARLY A DECADE AND THE ROLE DEFENDANT KEFFER AND UNIVERSITY PLAYED IN HIS SCHEME

17. Plaintiff brings this class action against Defendants University and Keffer for their failure to properly secure the highly sensitive personally identifiable information (“PII”) and

19. Upon information and belief, Defendant Loyola University Chicago contracted with Defendant Keffer.

21. Using the information that Weiss obtained from the student and student-athlete databases and his own research, Weiss was able to obtain access to the social media, email, and/or cloud storage accounts of more than 2,000 students. Defendant Weiss also illegally obtained access to the social media, email, and/or cloud storage accounts of more than 1,300 additional students and/or alumni from universities and colleges across the country. Once Weiss obtained access to these accounts, he downloaded personal, intimate digital photographs and videos that were never intended to be shared beyond intimate partners.

23. Through this scheme, unknown to students and student athletes, Defendant Weiss downloaded intimate digital photographs and videos.

24. This scheme appears to be the largest cyber sexual assault of student athletes in U.S. history.

25. The data breach and cyber sexual assault of over 150,000 students from university and college databases, including athletic databases maintained by Keffer, and the targeted exfiltration of intimate, personal, digital photographs and videos of 3,300 students and athletes, continued for nearly a decade because Defendant Loyola University Chicago and Defendant Keffer failed to prevent, detect, or stop Weiss from accessing those databases without and in excess of any authorization.

26. In at least several instances, Defendant Weiss exploited vulnerabilities in universities' account authorization processes to gain access to the accounts of students or alumni. Weiss then leveraged his access to these accounts to gain access to other social media, email, and/or cloud storage accounts.

27. That level of access through that number of accounts is an egregious and grossly negligent failure of data security on its face, as no institution with reasonable data security would allow such a breach over an eight-year period.

28. In March 2025, Matthew Weiss was charged in a 24-count indictment alleging 14 counts of unauthorized access to computers and 10 counts of aggravated identity theft, by the U.S. Attorney for the Eastern District of Michigan, for Weiss's perpetration of the cyber sexual assaults and data breach.

B. DEFENDANT KEFFER AND ITS “ATHLETIC TRAINER SYSTEM”

29. Defendant Keffer is a software development vendor that developed an electronic medical record system known as “The Athletic Trainer System,” which is used by many schools, colleges and universities across the United States.²

30. Defendant Keffer was founded in 1994 and currently collaborates with over 600 clients across 48 states and internationally.³ Defendant Keffer advertises that it currently serves over 6,500 schools, clinics, and other organizations with over 27,000 users and 2 million athletes.⁴

31. Upon information and belief, among the universities served by Keffer is Defendant University, Jane Doe 1’s alma mater.

32. Keffer represents that its Athletic Trainer System tool was “designed with athletic trainers for athletic trainers,” and is designed to store personal identifying information and personal health information belonging to students including their treatment histories, diagnoses, injuries, photos, and personal details, like height and weight, mental health information, and demographic information.⁵

33. In Keffer’s FAQ, it boasts that: “Keffer Development hosts all databases in our SSAE-16, SOC II and FedRamp certified data center” and that “Information security is a high priority in our company.”⁶ Keffer further claims that “On top of our Data Center being FedRamp Certified, ATS is also HIPAA and FERPA compliant. We utilize a company called Compliance Helper to ensure we maintain HIPAA and FERPA compliance.”⁷

² https://www.athletictrainersystem.com/pdf_files/Athlete_Info.pdf.

³ <https://www.athletictrainersystem.com/CompanyHistory.aspx>

⁴ <https://www.athletictrainersystem.com/Default.aspx>

⁵ See <https://www.athletictrainersystem.com/DemoRequest.aspx>

⁶ https://www.athletictrainersystem.com/pdf_Files/ATS_FAQ.pdf

⁷ *Id.*

34. In Keffer's Privacy Policy, it acknowledges that it has obligations as a "business associate" under HIPAA: "To the extent that KDS [Keffer] receives or maintains patient medical information in the course of providing the Clinical EMR, that information is secured, used and disclosed only in accordance with KDS' legal obligations as a "business associate" under HIPAA."⁸

35. Keffer's Privacy Policy further states: "KDS understands that storing our data in a secure manner is essential. KDS stores PII, PHI and other data using industry-standard physical, technical and administrative safeguards to secure data against foreseeable risks, such as unauthorized use, access, disclosure, destruction or modification. Please note, however, that while KDS has endeavored to create a secure and reliable website for users, the confidentiality of any communication or material transmitted to/from the Website or via e-mail cannot be guaranteed."⁹

36. Despite recognizing these obligations, Keffer failed to implement basic, industry standard systems to protect students' – including Jane Doe 1's personal identifying information and protected health information.

37. As an example, while Keffer maintained the option to incorporate two-factor authentication to access its Athletic Trainer System applications, it did not require that institutions and users do so.¹⁰ A two-factor basic security measure that requires an additional layer of authentication on top of a login credential, such as a code sent via text message or email – and critically, would have prevented Defendant Weiss from gaining access to student protected health information with only the access credentials belonging to other administrators and users.

⁸ https://www.athletictrainersystem.com/pdf_Files/ATS_Privacy_Policy.pdf

⁹ *Id.*

¹⁰ https://www.athletictrainersystem.com/pdf_Files/ATS_FAQ.pdf

38. Defendants knew that Keffer did not require institutions and users to use two-factor authorization to access the private information and communications accessible through its system, including information maintained in the Defendant Loyola University Chicago's facilities, and thus knowingly and deliberately permitted Plaintiff's confidential information and communications to be accessed, shared, and divulged without authorization from Plaintiffs.

39. Recent actions by the FTC underscore the gross negligence and failings of Keffer and Defendant Loyola University Chicago in failing to ensure that the Athletic Trainer System was configured to default to two-factor or multi-factor authentication for access to its systems containing personal identifying information and protected health information. In February 2023, the FTC published an article titled, *Security Principles: Addressing Underlying Causes of Risk in Complex Systems*. The article highlighted the importance of multi-factor authentication (MFA), stating: "Multi-factor authentication is widely regarded as a critical security practice because it means a compromised password alone is not enough to take over someone's account."¹¹

40. Additionally, the FTC's enforcement actions over the past five years further emphasize the critical and fundamental role MFA plays in an effective data security system, where the FTC has repeatedly obtained MFA as a form of injunctive relief in data security enforcement actions.¹²

41. Keffer also lacked any effective data auditing program to measure the download activity from its system, which would have allowed it to detect the massive, years-long data breach

¹¹<https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems>

¹² E.g., *In re: Equifax* (July 2019), <https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach>; *In re Drizly* (Oct. 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million>.

on its systems by Defendant Weiss and the resulting cyber sexual assault on Plaintiff Jane Doe 1 and those Class Members similarly situated.

42. Both Keffer and Defendant Loyola University Chicago had a responsibility and duty to protect the private data of student athletes stored within their database and to have mechanisms in place to prevent such a gross invasion of privacy as what occurred in this case.

43. The risk of identity theft and breaches of security to access users' private, personal, and confidential information is foreseeable within the University and Keffer's information technology systems, and the University and Keffer are well aware of the foreseeable risks of breaches, such as those alleged in this case, that are likely to occur if their practices in detecting, preventing, and mitigating such breaches are substandard.

C. DEFENDANT UNIVERSITY'S FAILURE TO SAFEGUARD ITS STUDENTS' PRIVATE INFORMATION FOR NEARLY A DECADE

44. Defendant Loyola University Chicago is an established high-level educational institution, with a diverse athletic program, enrolling approximately 300 student athletes at any one time in 16 different sports at the NCAA Division 1 level.

45. In maintaining its athletics department and programs, Loyola University Chicago provides its student athletes with athletic trainers.

46. The University had a responsibility and duty to oversee the University's operations, policies and procedures, and to care for and protect the University's students.

47. The University was required to ensure that students, such as Jane Doe 1, were not exposed to sexual predators who would invade their privacy.

48. The University failed in this duty by failing to take any reasonable action to prevent the harm caused to Jane Doe 1 and other Class Members as alleged in this Complaint.

49. This prolific and egregious breach and violation was entirely preventable by the University and Keffer. As noted in a criminal complaint filed by the U.S. Attorney for the Eastern District of Michigan, Defendant Weiss breached Keffer's systems and the systems of colleges and universities across this nation by exploiting passwords and other vulnerabilities in the systems and authentication processes of Keffer and these universities. On information and belief, neither the University nor Keffer required that its employees or students implement safeguards like multi-factor authentication to access accounts, a standard practice for all entities collecting personal identifying information, especially medical data and PHI (protected health information).

50. The breach and cyber assaults were a direct result of Defendant Loyola University Chicago's and Keffer's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Jane Doe 1 and Class Members PII and PHI, leaving the most sensitive and personal information of students, like Jane Doe 1, vulnerable to exploitation by malicious predators like Defendant Weiss.

51. Defendant Loyola University Chicago was grossly negligent on two fronts: (1) in its hiring and oversight of Defendant Keffer and its entrusting of students' PII and PHI in the care of Defendant Keffer, and (2) in its maintenance, oversight and security of its own internal databases of those internal systems to protect student PII and PHI.

52. The University took no reasonable actions to prevent this access despite its duties to students and has taken no reasonable actions to notify or rectify harm to the victims of Matthew Weiss's misconduct and predation.

53. Thousands of students still remain at risk because the University and Keffer have failed to undertake any reasonable review of how Jane Doe 1's private and personal information is stored, maintained, and who can access such information, and from where.

54. To this day, the University has not formally informed Class Members impacted by Weiss's cyber sexual assault and misconduct.

D. LOYOLA UNIVERSITY CHICAGO WAS NEGLIGENT IN HIRING/CONTRACTING WITH DEFENDANT KEFFER AND IN ENTRUSTING STUDENTS PII AND PHI TO KEFFER

55. Defendant Loyola University Chicago provided its student athletes medical treatment, including from athletic trainer employees of the University.

56. To facilitate that treatment, the University contracted with Keffer to use its Athletic Training System application, which required that student athletes provide the University and Keffer with sensitive PII and PHI.

57. When collecting that information, the University, like Keffer, accepted an obligation to protect that information under contract and statutory principles, including as a "business associate" under HIPAA.

58. Jane Doe 1 and others similar to her entrusted that the University and Keffer would safeguard her private information and ensure the security and confidentiality of her data.

59. The University and Keffer had, and continue to have, a duty to protect Jane Doe 1 and to take appropriate security measures to protect private, personal, medical and intimate information, communications, and images.

60. The University knowingly and deliberately permitted access to and divulging of Plaintiffs' stored communications through Keffer and failed to take reasonable action to ensure that Keffer protected the privacy of the sensitive information of Jane Doe 1 and others like her.

61. Upon information and belief, the University failed to properly investigate Keffer and Keffer's protocols, and failed to adequately monitor or establish safeguards for Keffer's work

67. Because Keffer and the University failed to implement basic, industry standard security measures, together these Defendants allowed an alleged sexual predator, ex-football coach Matthew Weiss, to access students', and in particular female student athletes', most sensitive information for nearly a decade.

68. All Defendants disregarded the rights of Jane Doe 1 and Class Members. The University and Keffer knowingly, intentionally, willfully, recklessly and/or negligently provided access to and/or divulged Plaintiffs' private communications stored in their facilities; failed to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failed to disclose that they did not have adequately robust computer systems and security practices to safeguard private information; failed to take standard and reasonably available steps to prevent the data breach and cyber assault; failed to properly train their staff and employees on proper security measures; failed to provide Jane Doe 1 and the Class Members prompt notice of the data breach and cyber assault.

69. Defendants Loyola University Chicago's and Keffer's conduct amounts to a violation of the duties they owed to Jane Doe 1 under common law and state and federal statutory law, rendering them liable to Jane Doe 1 and the Class Members for the harms caused by this egregious and preventable cyber sexual assault and invasion of privacy. Defendant Weiss is equally liable for the harms inflicted on Jane Doe 1 and the Class Members by his intentional hacking and exfiltration of their private information under tort and statutory law.

70. Jane Doe 1 and the putative Class Members are current and former students at Loyola University Chicago and other affected institutions in the United States that were specifically targeted by Weiss and harmed by the violation of their privacy.

71. Jane Doe 1 and the putative Class Members suffered injury because of Defendants' conduct. These injuries included: invasion and loss of privacy, loss of dignity, humiliation, embarrassment, and severe emotional distress.

72. Jane Doe 1 seeks to remedy these harms on behalf of herself and all similarly situated individuals whose private information was accessed by Weiss.

73. Jane Doe 1 seeks remedies including, but not limited to, compensatory damages, nominal damages, punitive damages, and reimbursement of out-of-pocket costs. Jane Doe 1 also seeks injunctive and equitable relief to prevent future injury on behalf of herself and the putative Class Members.

E. JANE DOE 1'S ALLEGATIONS

74. Plaintiff Jane Doe 1 is a former student athlete at Loyola University Chicago.

75. While in school at Loyola University Chicago, Jane Doe 1 participated in the Volleyball program while Defendant Weiss's data breach and cyber sexual assault was ongoing.

76. As a student athlete, Jane Doe 1 received treatment from the University's athletic trainer staff, requiring her to disclose information about her treatment, including height, weight, injuries, medications, treatment plans, and analysis on performance and recovery. To receive treatment, Jane Doe 1 was required to use the Keffer database, and the PII and PHI Jane Doe 1 disclosed was saved on the Keffer system.

77. As a student, Jane Doe 1 was required to disclose personal information to the University and was issued a university email where sensitive, personal information was stored.

78. Because Keffer and the University never implemented the security safeguards needed to protect Jane Doe 1's PII and PHI, Defendant Weiss compromised the PII and PHI belonging to every student whose information was saved by the University and/or Keffer's Athletic

Trainer System database, including, on information and belief, Jane Doe 1's private and personal information.

79. Defendant Weiss compromised all information that was saved in the University and/or Athletic Trainer System databases, including Plaintiff's treatment information, injury information, height, weight, and other highly sensitive information.

80. Jane Doe 1 has received notice from the U.S. Department of Justice Victim Notification System that she was identified as a potential victim in the federal action against Defendant Weiss.¹³

81. After receiving notice from the federal government that read: "If you are receiving this notification, it means that information of yours was found in possession of the defendant,"¹⁴ Jane Doe 1 felt violated, deeply disturbed, humiliated, embarrassed, and extremely emotionally distressed; and is experiencing physical manifestations of the stress and anxiety caused by this egregious violation of her privacy – symptoms that are further exacerbated by the fact that Jane Doe 1 still does not have a full and complete understanding of the data breach and cyber sexual assault perpetrated by Defendant Weiss.

82. This cyber sexual assault invaded Plaintiff's privacy and has devastated her personally and emotionally, as her highly sensitive private information was stolen by an alleged predator under circumstances that were entirely preventable by Defendant University and Defendant Keffer.

83. Upon information and belief, the United States Department of Justice is in the process of notifying thousands of potential victims that their privacy was breached.

¹³ See **Exhibit A**.

¹⁴ *Id.*

84. As a direct result of the negligence, recklessness, and misconduct of the Defendants, Jane Doe 1 and those similarly situated have incurred substantial monetary and emotional damages exceeding \$5,000,000, exclusive of costs, interest, and fees.

DEFENDANTS KEFFER AND LOYOLA UNIVERSITY
CHICAGO FAILED TO PROPERLY PROTECT PLAINTIFF'S AND CLASS
MEMBERS' PII AND PHI

85. Defendants Keffer and University did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted PII and PHI it was maintaining for Plaintiff and Class Members, causing the exposure of PII and PHI for 150,000 students and former students, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for approximately 3,330 students and former students.

86. The FTC promulgated numerous guides which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

87. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.¹⁵ The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone

¹⁵ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.¹⁶

88. The FTC further recommends that companies not maintain PII and PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

89. Defendants Keffer and Loyola University Chicago failed to properly implement basic data security practices explained and set forth by the FTC.

90. Defendants Keffer's and Loyola University Chicago's failure to employ reasonable and appropriate measures to protect against unauthorized access of PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

91. A systematic, years-long breach such as the ones Defendants Keffer and Loyola University Chicago experienced is also considered a breach under the HIPAA Rules because there is an unauthorized access to PHI that is not permitted under HIPAA.

92. A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." 45 C.F.R. 164.40.

93. Data breaches are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

¹⁶ *Id.*

The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. 45 C.F.R.164.308(a)(6).¹⁷

94. Defendants Keffer's and Loyola University Chicago's data breach was the foreseeable consequence of a combination of insufficiencies that demonstrate that Defendants Keffer and Loyola University Chicago failed to comply with safeguards mandated by HIPAA.

**DEFENDANTS LOYOLA UNIVERSITY CHICAGO AND KEFFER
FAILED TO COMPLY WITH INDUSTRY STANDARDS**

95. Defendants Keffer and Loyola University Chicago did not utilize industry standards appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of PII and PHI for approximately 150,000 students and former students, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for 3,330 students and former students.

96. As explained by the FBI, "[p]revention is the most effective defense against cyberattacks] and it is critical to take precautions for protection."¹⁸

97. To prevent and detect cyberattacks, including the cyberattack that resulted in this prolific data breach and cyber sexual assault, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of cyberattacks and how it is delivered.

¹⁷ *FACT SHEET: Ransomware and HIPPA*, U.S. Dept of Health and Hum. Servs., at 4 (July 11, 2016), <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>.

¹⁸ See How to Protect Your Networks from RANSOMWARE, at 3, <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Dec. 20, 2024).

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have written access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common cyberware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.¹⁹

98. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the data breach and cyber sexual assault, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the Internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . .
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it....
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

¹⁹ *Id.* at 3-4.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic....²⁰

99. To prevent and detect cyberattacks, including the cyberattack that resulted in the data breaches and cyber sexual assaults, Defendants Keffer and Loyola University Chicago could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure Internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection

²⁰ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), <https://www.cisa.gov/news-events/news/protecting-against-ransomware> (last visited Feb. 20, 2025).

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].²¹

100. As described above, experts studying cyber security routinely identify medical facilities as being particularly vulnerable to cyberattacks because of the value of the private information they collect and maintain.

101. Several best practices have been identified that at a minimum should be implemented by institutions such as Defendants Keffer and Loyola University Chicago, including, but not limited to, the following: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

102. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

103. Given that Defendants Keffer and Loyola University Chicago were storing the private information of 150,000 individuals combined, Defendants Keffer and Loyola University Chicago could and should have implemented all the above measures to prevent cyberattacks, along with the two-or multi-factor authentication discussed earlier in this Complaint.

²¹ See *Human-Operated Ransomware Attacks: A Preventable Disaster* (Mar 5, 2020), <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>.

104. The occurrence, scope and duration of the breach and cyber sexual assaults indicates that Defendants Keffer and Loyola University Chicago failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the exposure of approximately 150,000 students' and former students' PII and PHI, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for 3,330 students and former students.

DEFENDANTS KEFFER AND LOYOLA UNIVERSITY CHICAGO FAILED TO PROPERLY PROTECT PII AND PHI

105. Defendants Keffer and Loyola University Chicago breached their obligations to Jane Doe 1 and Class Members and were otherwise grossly negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches, cyber-attacks, hacking incidents, and ransomware attacks;
- b. Failing to adequately protect students' private information;
- c. Failing to properly monitor its own data security systems for existing or prior intrusions;
- d. Failing to test and assess the adequacy of its data security system;
- e. Failing to develop adequate training programs related to the proper handling of emails and email security practices;
- f. Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;
- g. Failing to require a data security system to ensure the confidentiality and integrity of electronic PHI its network created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

- h. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- i. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);
- j. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);
- k. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- l. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- m. Failing to ensure that it was compliant with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);
- n. Failing to train all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);
- o. Failing to ensure that the electronic PHI it maintained is unusable, unreadable, or indecipherable to unauthorized individuals, as Defendants had not encrypted the electronic PHI as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” (45 C.F.R. §164.304 definition of encryption);
- p. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;
- q. Failing to adhere to industry standards for cybersecurity.

106. As the result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendants Keffer and Loyola University Chicago negligently and unlawfully failed to safeguard Plaintiff’s and Class Members’ private, sensitive information.

107. Defendant Loyola University Chicago was also grossly negligent in its failure to oversee the data security practices of third-party vendor—Keffer—in which it entrusted the sensitive private information of its students and former students.

108. Accordingly, as outlined below, Plaintiff and Class Members have already been severely harmed by this egregious violation of their privacy by Defendant Weiss.

V. CLASS ALLEGATIONS

109. Plaintiff files this lawsuit both individually and as representative of all others similarly situated pursuant to Fed. R. Civ. P. 23 on behalf of the following Class:

All students whose personal data, images, information, social media, or videos were accessed by Weiss without authorization (the “Class Members”).

110. In addition, Plaintiff believes a subclass may be appropriate for all class members who receive notice from the United States Department of Justice as to the likely violation of their privacy and rights by Weiss. Therefore, Plaintiff pleads a subclass as follows:

All students whose personal data, images, information, social media, or videos were accessed by Weiss without authorization and who received a notice letter from the United States Department of Justice as to Weiss (the “DOJ Letter Sub-Class”).

111. Excluded from the Class are: (a) Defendants and any entity or division in which Defendants have a controlling interest, and their legal representatives, officers, directors, assigns, and successors; (b) the Judge to whom this case is assigned and the Judge’s staff; and (c) the attorneys representing any parties to this Class Action.

112. Plaintiff reserves the right to modify or amend the definition of the proposed class and/or sub-classes before the Court determines whether certification is appropriate.

NUMEROSITY – FED. R. CIV. P. 23(A)(1)

113. Law enforcement officials have disclosed the numbers of victims is significant and exceeds one thousand satisfying the numerosity requirement. Although the exact number of Class Members is uncertain at this time, it will certainly be ascertained through appropriate discovery, the number is great enough such that joinder is impracticable.

114. The members of the Class are so numerous and geographically disperse that individual joinder of all members is impracticable.

115. Similarly, Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

116. Class Members are readily identifiable from information and records in the possession of the federal and state authorities, the University, and Keffer.

117. Electronic records maintained by the University and Keffer can confirm the identification of Class Members.

COMMONALITY AND PREDOMINANCE – FED. R. CIV. P. 23(A)(2) AND 23(B)(3)

118. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and the other Class Members. Similar or identical violations, practices, and injuries are involved, and the burden of proof to establish violations of those rights involve uniform, objective questions of fact and law, both for the prosecution and for the defense.

119. The common questions of fact and law existing as to all Class Members predominate over questions affecting only individual class members. The evidence required to advance Plaintiff's and Class Members' claims are the same, common to all; as is true of the

evidence Defendants will likely rely upon in defense of this action. Thus, the elements of commonality and predominance are both met.

120. For example, establishing the facts of how, where, who, when, and through what means the invasions of Plaintiff's and other Class Members occurred are identical.

121. Defendants' actions, inactions, negligence, and recklessness apply commonly to Plaintiff and Class Members.

122. The downloads and invasions by Weiss and the improper conduct accessing private information through unsecure facilities without permission is common to all Class Members and has caused injury to the Plaintiff and Class Members in common manners.

123. The majority of legal and factual issues of the Plaintiff and the Class Members predominate over any individual questions, including:

- (a) Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members private information;
- (b) Whether Defendants Keffer and the University failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the hacking incident and cyber sexual assault;
- (c) Whether Defendants Keffer and the University's data security systems prior to and during the data breach and cyber sexual assault complied with applicable data security laws and regulations;
- (d) Whether Defendants Keffer's and the University's data security systems prior to and during the data breach and cyber sexual assault were consistent with industry standards;
- (e) Whether Defendants Keffer and the University owed a duty to Plaintiff and Class Members to safeguard their private information;
- (f) Whether Defendants Keffer and the University breached their duty to Plaintiff and Class Members to safeguard their private information;
- (g) Whether Defendant University was grossly negligent and/or negligent in its oversight of Defendant Keffer;

- (h) Whether Defendant University or Keffer knew or should have known that their data security systems and monitoring processes were deficient;
- (i) Whether Defendants Keffer and the University owed a duty to provide Plaintiff and Class Members timely notice of the data breach and cyber sexual assaults, and whether Defendants Keffer and the University breached that duty to provide timely notice;
- (j) Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;
- (k) Whether Defendants' conduct was negligent or grossly negligent;
- (l) Whether Defendants' conduct was per se negligent;
- (m) Whether Defendants' conduct violated federal laws;
- (n) Whether Defendants' conduct violated state laws;
- (o) Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or punitive damages; and
- (p) Other common questions of fact and law relative to this case that remain to be discovered.

124. Resolving the claims of these Class Members in a single action will provide benefit to all parties and the Court by preserving resources, avoiding potentially inconsistent results, and providing a fair and efficient manner to adjudicate the claims.

125. Predominance does not require Plaintiff to prove an absence of individualized damage questions, or even proof of class wide damage in the aggregate. *Kuchar v. Saber Healthcare Holdings LLC*, 340 F.R.D. 115, 123 (N.D.Ill. 2021) (finding individualized damages questions also do not defeat a predominance finding and noting "when adjudication of questions of liability common to the class will achieve economies of time and expense, the predominance standard is generally satisfied even if damages are not provable in the aggregate.").

TYPICALITY – FED. R. CIV. P. 23(A)(3)

126. Plaintiff’s claims are typical of those of other Class Members because all had their private information compromised as a result of the breach and cyber assault and Defendants’ malfeasance.

127. Plaintiff’s claims are typical of the Class Members because they are highly similar and the same and related in timing, circumstance, and harm suffered. To be sure, there are no defenses available to Defendants that are unique to individual Plaintiffs. The injury and causes of actions are common to the Class as all arising from the same statutory and privacy interests.

128. In *Halliburton Co. v. Erica P. John Fund, Inc.*, 573 U.S. 258, 276 (2014) the Supreme Court concluded that so long as plaintiffs could show that their evidence is capable of proving the key elements to plaintiffs’ claim on a class-wide basis, the fact that the defendants would have the opportunity at trial to rebut that presumption as to some of the plaintiffs did not raise individualized questions sufficient to defeat predominance. “That the defendant might attempt to pick off the occasional class member here or there through individualized rebuttal does not cause individual questions to predominate.” *Id.*

129. Certification of Plaintiff’s claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

130. The need to conduct additional post certification stage discovery, such as further file review or class member surveys, to eliminate uninjured persons after trial, does not act as a *de facto* bar to certification. *Nixon v. Anthem, Inc.*, 2021 WL 4037824, at *8 (E.D. Ky. Sept 1, 2021) (citing *Young v. Nationwide Mut. Ins. Co.*, 693 F.3d 532, 540 (6th Cir. 2012); *In re Visa Check/MasterMoney Antitrust Litig.*, 280 F.3d 124, 145 (2d Cir. 2001); *Perez v. First Am. Title*

Ins. Co., 2009 WL 2486003, at *7 (D. Ariz. Aug. 12, 2009) (“Even if it takes a substantial amount of time to review files and determine who is eligible for the [denied] discount, that work can be done through discovery.”); *Slapikas v. First Am. Title Ins. Co.*, 250 F.R.D. 232, 250 (W.D. Pa. 2008) (finding class action manageable despite First American's assertion that “no database exists easily and efficiently to make the determination that would be required for each file”).

131. Any remaining disputes on membership or class members damages can be left to a special master's decision. *Whitlock v. FSL Mgmt., LLC*, 2012 WL 3274973, at *12 (W.D. Ky., 2012), *aff'd*, 843 F.3d 1084 (6th Cir. 2016). By placing the validation of injury step at the end of the class trial process, no injured class members are left out, and at the same time, Defendants are not at risk for paying any uninjured class members.

ADEQUACY OF REPRESENTATION – FED. R. CIV. P. 23(A)(4)

132. Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that she has no interests that are in conflict with those of the Class Members. In addition, she has retained counsel competent and experienced in complex class action litigation, and she will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and her counsel.

SUPERIORITY OF CLASS TREATMENT – FED. R. CIV. P. 23(B)(3)

133. The class action is superior to any other available procedures for the fair and efficient adjudication of these claims, and no unusual difficulties are likely to be encountered in the management of this class action.

134. The superiority analysis required to certify a class is designed to achieve economies of time, effort and expense, and to promote uniformity of decisions as to persons similarly placed, without sacrificing procedural fairness or bringing about other undesirable results.

135. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable.

136. It would be an unnecessary burden upon the court system to require these individual Class Members to institute separate actions. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

137. Pursuing this matter as a class action is superior to individual actions because:

- (a) Separate actions by Class Members could lead to inconsistent or varying adjudications that would confront Defendants with potentially incompatible standards of conduct;
- (b) Many victims will not come forward without a certified class;
- (c) Final equitable relief will be appropriate with respect to the entire Class as a whole for monitoring, protection, therapy and other equitable forms of relief that may be provided;
- (d) This action is manageable as a class action and would be impractical to adjudicate any other way;
- (e) Absent the class action, individual Class Members may not know if their privacy was invaded; where such images are currently being stored, or are accessible by others; and their injuries are likely to go unaddressed and unremedied; and,
- (f) Individual Class members may not have the ability or incentive to pursue individual legal action on their own.

PARTICULAR ISSUES – FED. R. CIV. P. 23(c)(4)

138. In the event unforeseen issues preclude class certification under Fed.R.Civ.P. 23(b)(3), the case is still appropriate for class certification under Fed.R.Civ.P. 23(c)(4), as to the particular issues of liability.

139. Defendants have acted or refused to act on grounds generally applicable to Plaintiff and the other members of the Class, thereby making declaratory relief, as described below, with respect to the Class as a whole.

COUNT I
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT – 18 U.S.C. § 1030
(Defendant Weiss)

140. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

141. Plaintiffs allege that Defendant Weiss violated the Computer Fraud and Abuse Act.

142. Weiss violated the Computer Fraud and Abuse Act by unlawfully accessing Plaintiffs' private information without authorization.

143. Weiss' actions constituted a violation of the Act because by entering the digital network and extracting sensitive private information of students, he "intentionally accesse[d] a computer without authorization" and/or "exceed[ed] authorized access, and thereby obtain[ed] ... information." 18 U.S.C. § 1030(a)(2)(C).

144. Weiss's actions were deliberate because he knew he was unauthorized and proceeded nevertheless.

145. Under 18 U.S.C. § 1030(g), Plaintiffs may recover damages in this civil action from Weiss along with injunctive relief or other equitable relief.

146. Given the willful violations committed by Weiss, resulting in significant damage, harm, humiliation, and distress to Plaintiffs and other Class Members, Plaintiffs should be awarded all appropriate damages in this matter.

COUNT II
VIOLATIONS OF THE STORED COMMUNICATIONS ACT
18 U.S.C. § 2701 et seq
(Defendants Weiss, Loyola University Chicago, and Keffer)

147. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

148. Plaintiffs allege that Defendants Weiss, Keffer, and University violated the Stored Communications Act.

149. The Stored Communications Act, 18 U.S.C. § 2701 et seq., prohibits the unauthorized access of web-based cloud storage and media accounts such as those at issue and other accounts hosted by Defendants University and Keffer that contain personal, private, and intimate information and communications about and relating to Plaintiffs and others situated similarly to Plaintiffs.

150. Specifically, under 18 U.S.C. § 2701(a), it is unlawful for any person to: (1) intentionally access without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceed an authorization to access that facility; and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system.

151. Under 18 U.S.C. § 2702, it is unlawful for a person or entity providing an electronic communication service to the public to knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service or to divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of a subscriber or customer of such service, solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the

contents of any such communications for purposes of providing any services other than storage or computer processing.

152. Plaintiffs' electronic information and communications were in electronic storage and clearly fall within the scope of the statute.

153. Defendant Weiss was not authorized to access or divulge the content of Plaintiffs' private communications by for any purpose.

154. The information, messages, files, and media were accessed by Weiss without authorization.

155. Weiss's access without authorization were deliberate.

156. There is no manner in which Plaintiffs' private information, messages, files, and media could have been obtained without unauthorized access and would not have been obtained without unauthorized access had Defendants University and Keffer not knowingly divulged or permitted access to such information, through Keffer Development other channels, despite knowing that the information would not be protected.

157. Under Section 2707 of the Stored Communications Act, individuals may bring a civil action for the violation of this statute.

158. This law imposes strict liability on violators.

159. The statute provides that a person aggrieved by a violation of the act may seek appropriate relief including equitable and declaratory relief, actual damages or damages no less than \$1,000 punitive damages, and reasonable attorney's fee[s] and other litigation costs reasonably incurred according to 18 U.S.C. § 2707(b)-(c).

160. Defendants' access to and divulging of Plaintiffs' private, personal, and intimate information, messages, files, and media constituted a violation of 18 U.S.C. §§ 2701 and 2702.

161. The University, Keffer, and Weiss knew they did not have authority to access and divulge Plaintiffs' private, personal, and intimate information, messages, files, and media but did so anyway.

162. Defendants' knowing or intentional conduct led to multiple violations of the Stored Communications Act.

163. As a result of these violations, Plaintiffs have incurred significant monetary and nonmonetary damages as a result of these violations of the Stored Communications Act, and Plaintiffs seek appropriate compensation for their damages.

164. Under the statute, Plaintiffs should be granted the greater of (1) the sum of their actual damages suffered and any profits made by the University and Weiss as a result of the violations or (2) \$1,000 per violation of the Stored Communications Act.

165. Given these violations were deliberate, the Court should assess punitive damages against Defendants as well.

166. Plaintiffs should also be granted reasonable attorney fees and costs.

COUNT III
VIOLATION OF TITLE IX, 20 U.S.C. § 1681(A) Et Seq.
(Defendant Loyola University Chicago)

167. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

168. Plaintiffs allege that Defendant Loyola University Chicago violated Title IX, 20 U.S.C. § 1681(A) et seq.

169. Defendant Loyola University Chicago receives federal financial support for its educational programs and is therefore subject to the provisions of Title IX of the Education Act of 1972, 20 U.S.C. § 1681(a), et seq.

170. Title IX mandates that “No person in the United States shall on the basis of sex, be ... subject to discrimination under any education program or activity receiving Federal financial assistance ...”

171. Each Plaintiff and Class Member is a “person” under the Title IX statutory language.

172. Weiss specifically targeted women in his unwanted invasions of privacy and his misconduct is discrimination on the basis of sex.

173. Defendant Loyola University Chicago, under Title IX, is obligated to investigate allegations of sexual harassment.

174. Defendant Loyola University Chicago was aware of the sensitive nature of the private and personal information of Plaintiffs to which Weiss was able to access.

175. Defendant Loyola University Chicago acted with deliberate indifference to sexual harassment by:

- a. Failing to protect Plaintiffs and others as required by Title IX;
- b. Neglecting to adequately investigate and address the complaints regarding the deeply sensitive information Plaintiffs provided;
- c. Failing to institute corrective measures to prevent Weiss from sexually harassing students; and
- d. Failing to adequately investigate the other multiple acts of deliberate indifference.

176. Defendant Loyola University Chicago acted with deliberate indifference as their lack of response to the sexual harassment was clearly unreasonable in light of the known circumstances.

177. Defendant Loyola University Chicago's failure to promptly and appropriately protect, investigate, and remedy and respond to the sexual harassment of women has effectively denied them equal educational opportunities at the University, including access to medical care and sports training.

178. At the time the Plaintiffs received some medical and/or athletic training services from the University, they did not know the Defendant failed to adequately consider their safety.

179. As a result of Defendant Loyola University Chicago's deliberate indifference, Plaintiffs have suffered loss of educational opportunities and/or benefits.

180. Plaintiffs have incurred, and will continue to incur, attorney's fees and costs of litigation.

181. At the time of Defendants' misconduct and wrongful actions and inactions, Plaintiffs were unaware, and or with reasonable diligence could not have been aware, of Defendants' institutional failings with respect to their responsibilities under Title IX.

182. Defendant Loyola University Chicago maintained a policy and/or practice of deliberate indifference to protection of female student athletes.

183. Defendant's policy and/or practice of deliberate indifference to protection against the invasion of privacy for female athletes created a increased risk of sexual harassment.

184. Despite being able to prevent these privacy violations and acts of harassment, Defendant failed to do so.

185. Because of the Defendant Loyola University Chicago's policy and/or practice of deliberate indifference, Plaintiffs had their privacy invaded and were sexually harassed by Weiss.

187. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

188. Plaintiffs allege Defendant Weiss violated their civil rights under 42 U.S.C. § 1983 and the Fourth Amendment of the U.S. Constitution.

189. Defendant Weiss, sued in his individual capacity, was a state employee at all times relevant to this action, and acted under color of state law to deprive Plaintiffs of their “rights, privileges or immunities secured by the Constitution and laws” of the United States, 42 U.S.C. § 1983, specifically their Fourth Amendment right to be free warrantless and unreasonable searches and seizures.

190. At the time of his actions giving rise to this case, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally searched and seized Plaintiffs' private information without their consent, without a warrant, without probable cause or reasonable suspicion, and without any lawful basis or justification, in violation of Plaintiffs' clearly established rights under the Fourth Amendment.

191. The Fourth Amendment states: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.”

192. It is well settled that the Fourth Amendment's protection extends beyond the sphere of criminal investigations. *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 755 (2010) (citing *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 530 (1967)).

193. "The [Fourth] Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government," without regard to whether the government actor is investigating crime or performing another function." *Id.* (quoting *Skinner v. Railway Labor Executives' Assn.*, 489 U.S. 602, 613-614 (1989)).

194. Plaintiffs had a reasonable and legitimate expectation of privacy in their private, personal, and intimate information and images.

195. Acting under color of law, Defendant Weiss violated Plaintiffs' clearly established right not to have their private, personal, and intimate information and images. accessed, searched, viewed, and seized when he searched and seized Plaintiffs' private, personal, and intimate information and images without a warrant, without reasonable suspicion, without probable cause, and without any lawful basis, justification or need to support such an intrusion on Plaintiffs' reasonable and legitimate expectation of privacy in that information.

196. Defendant Weiss's search and seizure of Plaintiffs' personal information was per se unreasonable under the Fourth Amendment.

197. Defendant Weiss' search and seizure of Plaintiffs' private, personal, and intimate information and images was unjustified at its inception and was not related in scope to any circumstances that would justify the search and seizure in the first place.

198. Defendant Weiss is not entitled to qualified immunity because Plaintiffs' rights under the Fourth Amendment not to have their personal information searched and seized by him without a warrant, without permission, and without any lawful basis or justification, was obvious

and clearly established when Weiss accessed Plaintiffs' private information, such that no reasonable person in Weiss's position would believe that the act of searching and seizing Plaintiffs' private information was lawful under the specific circumstances presented, and Weiss had fair warning under the law as it existed at the time of his actions that those actions obviously violated Plaintiffs' rights under the Fourth Amendment.

199. As a direct and proximate result of Weiss's violation of Plaintiffs' Fourth Amendment rights, Plaintiffs have suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

200. Plaintiffs should be awarded all such forms of damages in this case for Weiss's conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

COUNT V
VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.
§ 1983 - DUE PROCESS/BODILY INTEGRITY
(Defendant Weiss)

201. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

202. Plaintiffs are alleging Defendant Weiss violated their civil rights under 42 U.S.C. § 1983 and the Fourteenth Amendment of the U.S. Constitution.

203. Defendant Weiss, sued in his individual capacity, was a state employee at all times relevant to this action, and acted under color of state law to deprive Plaintiffs of their "rights, privileges or immunities secured by the Constitution and laws" of the United States, 42 U.S.C. § 1983, specifically their Fourteenth Amendment equal protection right to be free from sexual harassment in an educational setting, and their Fourteenth Amendment due process right to be free

from violation of bodily integrity. *West v. Atkins*, 487 U.S. 42, 49-50 (1988) (quoting *Lugar v. Edmondson Oil Co.*, 457 U.S. 922, 936 n. 18 (1982)).

204. At the time of the actions giving rise to this case, it was obvious, clearly established, and known to Weiss that the right to be free from sexual abuse at the hands of a state employee was protected by the Due Process Clause of the Fourteenth Amendment, such that he knew his actions in accessing Plaintiffs' Plaintiffs' private, personal, and intimate information and images violated Plaintiffs' fundamental right of due process.

205. At the time of his actions giving rise to this case, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally engaged in actions which violated Plaintiffs' right of bodily integrity, in violation of the Due Process Clause.

206. Weiss's actions were malicious, intentionally harmful, and were taken with deliberate indifference, and were so outrageous as to shock the contemporary conscience.

207. As a direct and proximate result of Weiss's violation of Plaintiffs' Fourteenth Amendment rights, Plaintiffs have suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

208. Plaintiffs should be awarded all such forms of damages in this case for Weiss's conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

COUNT VI
VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.
§ 1983 - EQUAL PROTECTION
(Defendant Weiss)

209. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

210. Plaintiffs are alleging Defendant Weiss violated their civil rights under 42 U.S.C. § 1983 and the Fourteenth Amendment of the U.S. Constitution.

211. Weiss's deliberate and intentional actions in accessing Plaintiffs' personal, private, and intimate images and information constituted sexual harassment and abuse because Weiss accessed Plaintiffs' highly sensitive, private, and personal information, data, and media for his own personal and sexual purposes.

212. At the time of the actions giving rise to this case, it was obvious, clearly established, and known to Weiss that the right to be free from gender discrimination, including sexual harassment and abuse at the hands of a state employee, was protected by the Equal Protection Clause of the Fourteenth Amendment, such that Weiss knew his actions in accessing Plaintiffs' personal, private, and intimate images and information violated Plaintiffs' rights under the Fourteenth Amendment.

213. At the time of his actions giving rise to this case, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally engaged in sexual harassment and sexual abuse, in violation of the Equal Protection Clause.

214. As a direct and proximate result of Weiss's violation of Plaintiffs' Fourteenth Amendment rights, Plaintiffs have suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

215. Plaintiffs should be awarded all such forms of damages in this case for Weiss's conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

COUNT VII
VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.
§ 1983 - DUE PROCESS/DEPRIVATION OF PROPERTY
(Defendant Weiss)

216. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

217. Plaintiffs allege that Defendant Weiss violated their civil rights under 42 U.S.C. § 1983 and the Fourteenth Amendment of the U.S. Constitution.

218. Defendant Weiss, sued in his individual capacity, was a state employee at all times relevant to this action, and acted under color of state law to deprive Plaintiffs of their "rights, privileges or immunities secured by the Constitution and laws" of the United States, 42 U.S.C. § 1983, specifically their Fourteenth Amendment due process right to be free of deprivations of property without due process

219. At the time of the actions giving rise to this case, it was obvious, clearly established, and known to Weiss that the right not to be deprived of one's property without due process was protected by the Due Process Clause of the Fourteenth Amendment, such that he knew his actions in accessing and misappropriating Plaintiffs' private, personal, and intimate information and images violated Plaintiffs' fundamental right of due process.

220. Plaintiffs and others similarly situated had a protected property interest in their personal, private, intimate, and confidential information.

221. At the time of his actions giving rise to this case, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally engaged in actions which violated Plaintiffs' right not to be deprived of their personal property, in violation of the Due Process Clause.

222. Weiss' actions were malicious, intentionally harmful, and were taken with deliberate indifference, and were so outrageous as to shock the contemporary conscience.

223. As a direct and proximate result of Weiss' violation of Plaintiffs' Fourteenth Amendment rights, Plaintiffs have suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

224. Plaintiffs should be awarded all such forms of damages in this case for Weiss' conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

RELIEF

WHEREFORE, Plaintiff prays this Court grant the following relief:

- a. Enter a judgment encompassing the relief requested above, plus significant compensatory damages exceeding \$5,000,000.00 together with costs, interest and attorney fees, against Defendants, and such other relief to which they are entitled;
- b. An order certifying the proposed Class and Subclasses; designating Plaintiff as the named representative of the respective Class Members; and appointing her counsel as Class Counsel;
- c. All such equitable relief as the Court deems proper and just, including but not limited to, declaratory relief;
- d. Award Plaintiff costs, attorney fees as well as interest from the date of Judgment until paid; and
- e. Grant such further relief as is agreeable to equity and good conscience.

JURY DEMAND

For all triable issues, a jury is hereby demanded.

Respectfully Submitted,

/s/ Edward A. Wallace

Edward A. Wallace

Jacob Podell

WALLACE MILLER

150 North Wacker Drive, Suite 1100

Chicago, IL 60606

T: 312.261.6193

F: 312.275.8174

E: eaw@wallacemiller.com

jpodell@wallacemiller.com

Counsel for Plaintiff and the Proposed Class

EXHIBIT A

REDACTED

F

[REDACTED]

[REDACTED]

[REDACTED]

----- Forwarded message -----

From: U.S. Department of Justice - VNS <fedemail@vns.usdoj.gov>

Date: Sun, Nov 10, 2024 at 3:00 PM

Subject: U.S. Department of Justice - VNS - Investigative Case 288A-DE-3728795

To: [REDACTED]

DO NOT REPLY TO THIS EMAIL.



November 10, 2024

U.S. Department of Justice
Federal Bureau of Investigation
Detroit Division
477 Michigan Ave
26th Floor
Detroit, MI 48226
Phone: DE-CYVictim@fbi.gov
Email: DE-CYVictim@fbi.gov

[REDACTED]

RE: Case Number: 288A-DE-3728795

Dear [REDACTED]:

As a Victim Specialist with the Federal Bureau of Investigation (FBI), Victim Services Division (VSD), Detroit Division, I am contacting you because you have been identified as a possible victim of a federal crime. The FBI is responsible for ensuring that victims receive information and services during the investigation of a federal crime while being treated with dignity and respect.

As a possible victim of a federal crime, you are legally entitled to receive certain services and assistance including notifications on the case listed above. We will make every effort to keep you informed about the case to the extent that we can while not interfering with the investigation. We are also committed to providing you with support and information about available services, programs, and resources. Please contact me if you would like information or referrals for services in your area.

Throughout the investigation you may receive multiple notifications. The purpose of this initial letter is to notify you that this case is currently under investigation. If the

investigation results in the filing of federal charges, notifications will be sent to you by the United States Attorney's Office.

If you have questions about this notification or would like information about available resources, you can contact DE-CYVictim@fbi.gov. If you would like to verify the legitimacy of this notification, please contact the FBI Detroit Field Office at (313) 965-2323. You can also find this phone number listed on FBI Detroit's website.

Due to the large number of potential victims in this case, you will likely not receive additional correspondence by mail. Updates will continue to be available in VNS, through your profile or by email. VNS must have an email address on file to send updates and notifications by email. You can verify or enter your email address by logging into VNS and updating your contact information.

Below you will find information on the Victim Notification System (VNS). VNS is designed to keep victims informed about their case. The system incorporates outgoing notifications such as this letter, a call center, and an online tool. The call center and online tool also allow you to update your contact information and notification preferences. Through VNS, please remember that you may choose to stop or resume notifications at any time. Given the sensitivity of some information, case status information available through VNS may be very limited. Lastly, if you wish to receive important notifications in your case, it is your individual responsibility to maintain current contact information in the system.

Current information regarding the status of your case can be found on the Internet at <https://www.notify.usdoj.gov> or by calling the Victim Notification System (VNS) Call Center at 1-866-DOJ-4YOU (1-866-365-4968). You will need to enter your Victim Identification Number (VIN) [REDACTED] and your Personal Identification Number (PIN) [REDACTED] anytime you contact the Call Center and the first time you log into VNS on the Internet. If you are receiving notifications with multiple victim ID/PIN codes please contact the VNS Call Center. In addition, the first time you access the VNS Internet site, you will be prompted to enter your last name (or business name) as currently contained in VNS. The name you should enter is [REDACTED].

You can also use the Call Center and the Internet to correct/update your contact information and/or change your decision regarding participation in the notification system. Your participation in this notification system is totally voluntary. You can choose not to participate or reactivate your access at any time. In order to continue to receive notifications, it is your responsibility to keep your contact information current.

The email address VNS currently has for you is [REDACTED]. If this address is correct and you have not received an email from VNS within four days of the date of this letter, please check your junk/spam folder and accept emails from fedemail@vns.usdoj.gov. If the email address provided above is incorrect, please update the email address by accessing the VNS Web site. This email address has not been verified in VNS and future emails will not contain details about the nature of the notification. To receive subsequent emails with the full text of the notification you must verify this email address by accessing the VNS Internet web page using the login information provided above.

Once you have verified/updated your email address, most, if not all, future notifications will be provided by email and not by letter. If you do not verify your email address, VNS will

continue (in most cases) to send letter and email notifications. However, when an email address is not verified, future emails will not contain details about the nature of the notification.

If you have additional questions related to this matter, please contact me at DE-CYVictim@fbi.gov. When you call, please provide the file number located at the top of this letter.

Sincerely,

Nicole McGee
Victim Specialist

If you do not want to receive email notifications from the Victim Notification System (VNS) please log into the VNS Web site at <https://www.notify.usdoj.gov>, select "My Information", remove your email address and click the "update" button. If you remove your email address, you will continue to receive letters from VNS except in those case which have large numbers of victims. To change your email address, select "My Information", provide a new address and click the "update" button.

If you do not want to receive any notifications in your case, select "Stop Receiving Notifications" and follow the instructions on the screen.

If you believe you have received this email in error, please contact the office listed at top of the email message.

Please note, if this is the first notification you have received from VNS you will need to wait 4-8 hours from receipt of this email before you can login to the VNS Internet site (<https://www.notify.usdoj.gov>). In addition, it will also be 4-8 hours before any documents which may have been uploaded to VNS as part of this notification are available under the "Downloads/Links" section on the Web page.

Please call the Victim Notification System (VNS) Help Desk at phone number 1-866-625-1631 for assistance and questions.

Attachments have been referenced with this notification and are available on the VNS Internet site (or will be available within 8 hours). After you log into the website select "Downloads/Links" to view the attachments.

[Query](#)[Reports](#)[Utilities](#)[Help](#)[Log Out](#)

Cat08,Knapp

**U.S. District Court
NORTHERN DISTRICT OF OHIO (Akron)
CIVIL DOCKET FOR CASE #: 5:25-cv-00827-SL**

Doe v. Weiss et al.
Assigned to: Chief District Judge Sara Lioi
Cause: 28:1331 Fed. Question

Date Filed: 04/24/2025
Jury Demand: Plaintiff
Nature of Suit: 360 P.I.: Other
Jurisdiction: Federal Question

Plaintiff**Jane Doe**

*I, individually and on behalf of all similarly
situated,*

represented by **Anna R. Caplan**
Barkan Meizlish DeRose Cox - Columbus
Ste. 210
4200 Regent Street
Columbus, OH 43082
614-221-4221
Fax: 614-744-2300
Email: acaplan@barkanmeizlish.com
ATTORNEY TO BE NOTICED

Jason J. Thompson
Sommers Schwartz - Southfield
Ste. 1700
One Towne Square
Southfield, MI 48076
248-355-0300
Email: jthompson@sommerspc.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

Kevin M. Carlson
Pitt McGehee Palmer Bonanni & Rivers -
Royal Oak
Ste. 200
117 West Fourth Street
Royal Oak, MI 48067
248-398-9800
Fax: 248-298-7996
Email: kcarlson@pittlawpc.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

Lisa M. Esser
Sommers Schwartz - Southfield
Ste. 1700
One Towne Square
Southfield, MI 48076

248-355-0300

Email: lesser@sommerspc.com

PRO HAC VICE

ATTORNEY TO BE NOTICED

Matthew G. Curtis

Sommers Schwartz - Southfield

17th Floor

One Towne Square

Southfield, MI 48076

248-746-4038

Fax: 248-936-2124

Email: mcurtis@sommerspc.com

PRO HAC VICE

ATTORNEY TO BE NOTICED

Megan A. Bonanni

Pitt McGehee Palmer & Rivers - Royal Oak
Ste. 200

117 West Fourth Street

Royal Oak, MI 48067

248-398-9800

Fax: 248-268-7996

Email: mbonanni@pittlawpc.com

PRO HAC VICE

ATTORNEY TO BE NOTICED

Richard L. Groffsky

Sommers Schwartz - Southfield

Ste. 1700

One Towne Center

Southfield, MI 48076

248-746-4028

Email: rgroffsky@somerspc.com

PRO HAC VICE

ATTORNEY TO BE NOTICED

Robert E. DeRose , II

Barkan Meizlish DeRose Cox

Ste. 210

4200 Regent Street

Columbus, OH 43219

614-221-4221

Fax: 614-744-2300

Email: bderose@barkanmeizlish.com

ATTORNEY TO BE NOTICED

V.

Defendant

Matthew Weiss

Defendant

Malone Universityrepresented by **Melissa Bilancini**

Baker & Hostetler - Cleveland

Ste. 2000

127 Public Square

Cleveland, OH 44114

216-621-0200

Fax: 216-696-0740

Email: mbilancini@bakerlaw.com

*ATTORNEY TO BE NOTICED***Defendant****Keffer Development, LLC**

Date Filed	#	Docket Text
04/24/2025	<u>1</u>	Class Action Complaint with jury demand against Keffer Development, LLC, Malone University, Matthew Weiss. Filing fee paid \$ 405.00, Receipt number AOHND-13066783. Filed by Jane Doe,1 individually and on behalf of all individuals similarly situated. (Attachments: # <u>1</u> Exhibit A-DOJ Letter, # <u>2</u> Civil Cover Sheet) (DeRose, Robert) (Entered: 04/24/2025)
04/24/2025		Judge Pamela A. Barker assigned to case. (B,Ch) (Entered: 04/24/2025)
04/24/2025		Random Assignment of Magistrate Judge pursuant to Local Rule 3.1. In the event of a referral, case will be assigned to Magistrate Judge Jonathan D. Greenberg. (B,Ch) (Entered: 04/24/2025)
04/24/2025	<u>2</u>	Magistrate Consent Form issued. Summons not provided and was not issued. (B,Ch) (Entered: 04/24/2025)
04/24/2025		Order [non-document] Counsel and the parties are hereby advised that this Court will not accept ex parte telephone calls to Chambers regarding substantive issues in pending cases. The Court speaks through its docket. While it may be appropriate to call Chambers regarding routine, non-substantive matters (such as requests for the dial in information for an upcoming status conference, etc.), it is not appropriate under any circumstances for counsel to call Chambers ex parte for guidance or clarification regarding substantive matters, including matters relating to existing case management deadlines, requests to file briefing, and/or inquiries regarding the status of pending motions. All questions regarding substantive matters in pending cases must be filed as a motion on the public docket, with the following exception. If a dispute arises during a deposition that requires this Court's immediate assistance, the parties may call Chambers for assistance, but must do so jointly (and not on an ex parte basis). Judge Pamela A. Barker on 4/24/2025. (P,K) (Entered: 04/24/2025)
04/24/2025	<u>3</u>	Supplement - Summons in a Civil Action, filed by Jane Doe. (Attachments: # <u>1</u> Keffer Development, LLC Summons) (DeRose, Robert) (Entered: 04/24/2025)
04/28/2025	<u>4</u>	Waiver of Service Returned Executed by Jane Doe. Malone University waiver sent on 4/28/2025, answer due 6/27/2025 filed on behalf of Jane Doe (DeRose, Robert) (Entered: 04/28/2025)
04/29/2025		Order [non-document] The Clerk's Office has indicated that there was an error in the assignment of this case; therefore, the case is being returned to the Clerk's Office for proper assignment. Judge Pamela A. Barker on 4/29/2025. (P,K) (Entered: 04/29/2025)

04/29/2025		Chief District Judge Sara Lioi assigned to case Judge Pamela A. Barker terminated. (B,Ch) (Entered: 04/29/2025)
04/29/2025		Reassignment of Magistrate Judge pursuant to Local Rule 3.1. In the event of a referral, case will be assigned to Magistrate Judge Amanda M. Knapp. (B,Ch) (Entered: 04/29/2025)
04/29/2025	5	Original Summons and Magistrate Consent Form issued to counsel for service upon Keffer Development, LLC, Malone University. (Attachments: # 1 Magistrate Consent Form) (B,Ch) (Entered: 04/29/2025)
04/30/2025	6	Attorney Appearance by Melissa Bilancini filed by on behalf of Malone University. (Bilancini, Melissa) (Entered: 04/30/2025)
04/30/2025	7	Motion for Appointment of Interim Class Counsel filed by Plaintiff Jane Doe. (Attachments: # 1 Exhibit 1-Weiss Indictment, # 2 Exhibit 2-Illinois Complaint, # 3 Exhibit 3-California Complaint, # 4 Exhibit 4-Maryland Complaint, # 5 Exhibit 5-NC Complaint, # 6 Exhibit 6-Motion for CMC, # 7 Exhibit 7-CMC Order, # 8 Exhibit 8-JD v. Weiss et al., Meet Confer Agenda 4.28.25, # 9 Exhibit 9-S2 Leadership Bios, # 10 Exhibit 10-Pitt Leadership Bios, # 11 Exhibit 11-Barkan Meizlish DeRose Cox Bio, # 12 Proposed Order 12-Proposed Order)(DeRose, Robert) (Entered: 04/30/2025)
05/02/2025	8	Waiver of Service Returned Executed by Jane Doe. Keffer Development, LLC waiver sent on 5/2/2025, answer due 7/1/2025 filed on behalf of Jane Doe (DeRose, Robert) (Entered: 05/02/2025)
05/06/2025		Service by Clerk. Summons and Complaint addressed to Keffer Development, LLC placed in U.S. Mail. Type of service: Certified mail. Receipt # 9589071052702138515798. (Gi,J) (Entered: 05/06/2025)
05/13/2025	9	Motion for attorney Richard L. Groffsky to Appear Pro Hac Vice. Filing fee \$ 120, receipt number AOHND-13097459, filed by Plaintiff Jane Doe. (Attachments: # 1 Exhibit Certificate of Good Standing)(DeRose, Robert) (Entered: 05/13/2025)
05/13/2025	10	Motion for attorney Jason J. Thompson to Appear Pro Hac Vice. Filing fee \$ 120, receipt number AOHND-13098063, filed by Plaintiff Jane Doe. (Attachments: # 1 Exhibit Certificate of Good Standing)(DeRose, Robert) (Entered: 05/13/2025)
05/14/2025		Order [non-document] granting plaintiff's motions (Doc. Nos. 9 and 10 for appearance pro hac vice by attorneys Richard L. Groffsky and Jason J. Thompson for Jane Doe. Local Rule 5.1(c) requires that attorneys register for NextGen CM/ECF and file and receive all documents electronically. NextGen CM/ECF registration can be done online at www.pacer.gov . Login with your PACER credentials, go to the Maintenance tab, click Attorney Admissions/E-File Registration, select Ohio Northern District Court and then select Pro Hac Vice. If you were previously granted pro hac vice status and are already registered to file electronically, it is not necessary to register again. Chief District Judge Sara Lioi on 5/14/2025. (V,A) (Entered: 05/14/2025)
05/14/2025	11	Motion for attorney Megan A. Bonanni to Appear Pro Hac Vice. Filing fee \$ 120, receipt number AOHND-13099564, filed by Plaintiff Jane Doe. (Attachments: # 1 Exhibit Certificate of Good Standing)(DeRose, Robert) (Entered: 05/14/2025)
05/14/2025	12	Motion for attorney Kevin M. Carlson to Appear Pro Hac Vice. Filing fee \$ 120, receipt number AOHND-13099571, filed by Plaintiff Jane Doe. (Attachments: # 1 Exhibit Certificate of Good Standing)(DeRose, Robert) (Entered: 05/14/2025)
05/14/2025	13	Motion for attorney Lisa M. Esser to Appear Pro Hac Vice. Filing fee \$ 120, receipt number AOHND-13100069, filed by Plaintiff Jane Doe. (Attachments: # 1 Exhibit

		Certificate of Good Standing)(DeRose, Robert) (Entered: 05/14/2025)
05/14/2025	14	Motion for attorney Matthew G. Curtis to Appear Pro Hac Vice. Filing fee \$ 120, receipt number AOHNDC-13100090, filed by Plaintiff Jane Doe. (Attachments: # 1 Exhibit Certificate of Good Standing)(DeRose, Robert) (Entered: 05/14/2025)
05/15/2025	15	Return of Service by Clerk by certified mail executed upon Keffer Development, LLC on 5/12/2025, filed on behalf of Jane Doe. Related document(s) 5 . (Gi,J) (Entered: 05/15/2025)
05/15/2025		Order [non-document] granting plaintiff's motions (Doc. Nos. 11 , 12 , 13 , and 14) for appearance pro hac vice by attorneys Megan A. Bonanni, Kevin M. Carlson, Lisa Michelle Esser, and Matthew G. Curtis for Jane Doe. Local Rule 5.1(c) requires that attorneys register for NextGen CM/ECF and file and receive all documents electronically. NextGen CM/ECF registration can be done online at www.pacer.gov. Login with your PACER credentials, go to the Maintenance tab, click Attorney Admissions/E-File Registration, select Ohio Northern District Court and then select Pro Hac Vice. If you were previously granted pro hac vice status and are already registered to file electronically, it is not necessary to register again. Chief District Judge Sara Lioi on 5/15/2025. (V,A) (Entered: 05/15/2025)
05/21/2025	16	Praeipie for issuance of Original Summons filed by Jane Doe. (Attachments: # 1 Summons to be Issued by the Clerk)(DeRose, Robert) (Entered: 05/21/2025)
05/27/2025	17	Original Summons issued to counsel for service upon Matthew Weiss. (B,DL) (Entered: 05/27/2025)
05/30/2025	18	Memorandum Opinion and Order denying without prejudice plaintiff's motion (Doc. No. 7) for the appointment of interim class counsel. Chief District Judge Sara Lioi on 5/30/2025. (V,A) (Entered: 05/30/2025)
06/03/2025		Service by Clerk. Summons and Complaint addressed to Matthew Weiss placed in U.S. Mail. Type of service: Certified mail. Receipt # 9414 7266 9904 2172 0942 95. (C,K) (Entered: 06/03/2025)
06/05/2025	19	Motion for attorney Edward J. McAndrew to Appear Pro Hac Vice. Filing fee \$ 120, receipt number AOHNDC-13134879, filed by Defendant Malone University. (Attachments: # 1 Exhibit Declaration in Support of Motion)(Bilancini, Melissa) (Entered: 06/05/2025)

PACER Service Center			
Transaction Receipt			
06/05/2025 16:16:15			
PACER Login:	ThomaKingtking	Client Code:	
Description:	Docket Report	Search Criteria:	5:25-cv-00827-SL
Billable Pages:	4	Cost:	0.40

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
CLEVELAND DIVISION**

**JANE DOE 1, individually and on
behalf of all individuals similarly situated,**

Plaintiffs,

V.

MATTHEW WEISS,

MALONE UNIVERSITY, and

KEFFER DEVELOPMENT, LLC,

Defendants.

CASE NO.:

JUDGE: _____

JURY DEMANDED

PLAINTIFF'S CLASS ACTION COMPLAINT

Plaintiff JANE DOE 1, through her attorneys, Sommers Schwartz, P.C., Pitt McGehee Palmer Bonanni & Rivers, P.C., and Barkan Meizlish DeRose Cox, LLP, for their Complaint against MATTHEW WEISS, MALONE UNIVERSITY, and KEFFER DEVELOPMENT SERVICES, LLC, states as follows:

I. INTRODUCTION

Students and alumni connected to Malone University from 2015 to 2023—many of them student-athletes—have been subjected to a deeply troubling and unlawful breach of privacy, stemming from the actions of former University of Michigan and Baltimore Ravens football coach Matthew Weiss, whose gross and despicable violations of their privacy were facilitated by institutional negligence. This class action lawsuit, filed against Matthew Weiss, Malone University, and Keffer Development Services, LLC, seeks justice for the unauthorized access and misuse of personal information—an abuse so severe that Malone University students and student-

athletes are now receiving formal notification from the U.S. Department of Justice that their private information, including intimate photos and videos, have been exposed, including Plaintiff Jane Doe 1. This action is brought to hold the Defendants accountable for failing to protect their students from foreseeable harm.

Plaintiff Jane Doe 1, on behalf of herself and all others similarly situated, brings federal claims pursuant to 18 U.S.C. § 1030 et seq, 18 U.S.C. § 2701 et seq., Title IX, 20 U.S.C. § 1681(A) et seq., 42 U.S.C. § 1983 et seq., the Fourth Amendment of the U.S. Constitution, and the Fourteenth Amendment of the U.S. Constitution against Defendants (the “federal claims”). Plaintiff Jane Doe 1, on behalf of herself and all others similarly situated, brings Ohio claims pursuant to Ohio Revised Code § 2917.211, Ohio Revised Code § 1349.19, Ohio Revised Code § 2913.49, and Ohio Revised Code § 2307.60 against Defendants (the Ohio Statutory Claims”). Plaintiff Jane Doe 1, on behalf of herself and all others similarly situated, brings Ohio claims for invasion privacy by intruding upon their seclusion, gross negligence, negligence, negligence *per se*, breach of implied contract, unjust enrichment, trespass to chattels, assault, and intentional infliction of emotional distress pursuant to Ohio common law against Defendants (the “Ohio Common Law Claims”).

II. PARTIES

1. Plaintiff Jane Doe 1 was a student athlete at Malone University between 2017 and 2022, and was a member of the school’s swim team.

2. Plaintiff Jane Doe 1 is domiciled in Cuyahoga County, Ohio, in the City of Cleveland.

3. In late March 2025, Plaintiff Jane Doe 1 received notice from the United States Department of Justice Victim Notification System that she was identified as a victim in the

criminal case against University of Michigan’s Coach Weiss: *United States v. Defendant(s) Matthew Weiss*.¹

4. Defendant Malone University (“University”) is a private university in Canton, Ohio (Stark County).

5. Malone University enrolls approximately 1,500 undergraduate and graduate students.

6. Malone University is a member of the National Collegiate Athletic Association (NCAA), with approximately 399 student athletes competing in 19 intercollegiate sports at the Division 2 level.

7. Defendant Keffer Development Services, LLC (“Keffer”) is a Pennsylvania limited liability company in Grove City, PA, that has continuously and systemically conducted business in Ohio by directly providing services to residents and entities within the State of Ohio, including its business contacts with Malone University in Canton, Ohio, thereby availing itself of protections of the law of the State of Ohio.

8. Defendant Keffer is a technology and data vendor operating an electronic medical record and student athlete training system, which stored the personal identifying information (“PII”) and personal health information (“PHI”) of Plaintiff and Class Members across the country.

9. Any wrongful conduct and legal violations committed by Defendant Keffer that are subsequently outlined in this Complaint occurred specifically with respect to the Plaintiff during the time of the incident alleged in this Complaint.

¹ Jane Doe 1’s DOJ Data Breach Notice is attached hereto as **Exhibit A**.

10. Matthew Weiss (“Weiss”) is an individual residing in the State of Michigan, who had contacts with the State of Ohio in that he conducted illegal activity in the State of Ohio, by hacking into the personal property of Plaintiff and putative Class Members of the State of Ohio during the applicable time period at issue in this Complaint and said activities from which this Complaint arises.

11. On March 20, 2025, Defendant Weiss was indicted on 24 counts of unauthorized access to computers and aggravated identity theft by the U.S. Attorney for the Eastern District of Michigan.

III. JURISDICTION AND VENUE

12. Jurisdiction is proper in this Court under 28 U.S.C. §§ 1331 and 1367 as this matter involves a claim under the Stored Communications Act, 18 U.S.C. § 2701(a) *et seq.*; the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; Title IX, 20 U.S.C. § 1681(A) *et seq.*; 42 U.S.C. § 1983; the Fourth Amendment of the U.S. Constitution; and the Fourteenth Amendment of the U.S. Constitution, and this Court has supplemental jurisdiction of all additional causes of action alleged in this Complaint pursuant to 28 U.S.C. §1367(a).

13. This Court also has subject matter jurisdiction pursuant to 28 U.S.C. §1332(d) under the Class Action Fairness Act (“CAFA”) as a class action lawsuit in which the amount in controversy exceeds \$5,000,000.00, there are more than one-hundred putative Class Members, and the majority of the putative Class Members are citizens of a state different than the state of which Defendants are citizens.

14. This Court has jurisdiction pursuant to 28 U.S.C. § 1367 over the Ohio Statutory Claims and the Ohio Common Law Claims.

15. The Court has personal jurisdiction over Defendants named in this action because Defendant University is located and created under the laws of the State of Ohio, and Defendant Weiss had minimum contacts with the State of Ohio as set in this Complaint, thus purposefully availing himself of the privilege of conducting activities in the State of Ohio. Defendant Keffer conducts business at the State of Ohio and has availed itself of the protections of Ohio state law. The claims at issue in this case arise out of Defendants’ purposeful contacts with and business activities in the State of Ohio.

16. Venue is appropriate in this District Court under 28 U.S.C. §1391(b) since a substantial part of the events or omissions giving rise to these claims occurred within this District.

17. Plaintiff’s injuries are redressable by monetary compensation, and all alleged injuries of Plaintiff and Class Members can be traced to Defendants’ conduct.

IV. COMMON ALLEGATIONS

A. WEISS’S DATA BREACH AND CYBER SEXUAL ASSAULT OF THOUSANDS OF STUDENTS FOR NEARLY A DECADE AND THE ROLE DEFENDANT KEFFER AND UNIVERSITY PLAYED IN HIS SCHEME

18. Plaintiff brings this class action against Defendants University and Keffer for their failure to properly secure the highly sensitive personally identifiable information (“PII”) and protected health information (“PHI”) of more than 150,000 students, including herself, which was targeted, accessed, and exfiltrated by former University of Michigan and Baltimore Ravens coach and sexual predator Matthew Weiss, over the course of nearly a decade.

19. Between 2015 and January 2023, Defendant Weiss gained unauthorized access to both student databases and student-athlete databases of more than 100 colleges and universities, some of which were maintained by Defendant Keffer, a third-party vendor contracted by these colleges and universities.

20. Upon information and belief, Defendant Malone University contracted with Defendant Keffer.

21. After gaining access to these databases, Weiss downloaded the PII and PHI of more than 150,000 athletes.

22. Using the information that Weiss obtained from the student and student-athlete databases and his own research, Weiss was able to obtain access to the social media, email, and/or cloud storage accounts of more than 2,000 students. Defendant Weiss also illegally obtained access to the social media, email, and/or cloud storage accounts of more than 1,300 additional students and/or alumni from universities and colleges across the country. Once Weiss obtained access to these accounts, he downloaded personal, intimate digital photographs and videos that were never intended to be shared beyond intimate partners.

23. Defendant Weiss primarily targeted female college athletes. He researched and targeted these women based on their school affiliation, athletic history, and physical characteristics.

24. Through this scheme, unknown to students and student athletes, Defendant Weiss downloaded intimate digital photographs and videos.

25. This scheme appears to be the largest cyber sexual assault of student athletes in U.S. history.

26. The data breach and cyber sexual assault of over 150,000 students from university and college databases, including athletic databases maintained by Keffer, and the targeted exfiltration of intimate, personal, digital photographs and videos of 3,300 students and athletes, continued for nearly a decade because Defendant Malone University and Defendant Keffer failed

to prevent, detect, or stop Weiss from accessing those databases without and in excess of any authorization.

27. In at least several instances, Defendant Weiss exploited vulnerabilities in universities' account authorization processes to gain access to the accounts of students or alumni. Weiss then leveraged his access to these accounts to gain access to other social media, email, and/or cloud storage accounts.

28. That level of access through that number of accounts is an egregious and grossly negligent failure of data security on its face, as no institution with reasonable data security would allow such a breach over an eight-year period.

29. In March 2025, Matthew Weiss was charged in a 24-count indictment alleging 14 counts of unauthorized access to computers and 10 counts of aggravated identity theft, by the U.S. Attorney for the Eastern District of Michigan, for Weiss's perpetration of the cyber sexual assaults and data breach.

B. DEFENDANT KEFFER AND ITS "ATHLETIC TRAINER SYSTEM"

30. Defendant Keffer is a software development vendor that developed an electronic medical record system known as "The Athletic Trainer System," which is used by many schools, colleges and universities across the United States.²

31. Defendant Keffer was founded in 1994 and currently collaborates with over 600 clients across 48 states and internationally.³ Defendant Keffer advertises that it currently serves over 6,500 schools, clinics, and other organizations with over 27,000 users and 2 million athletes.⁴

² https://www.athletictrainersystem.com/pdf_files/Athlete_Info.pdf.

³ <https://www.athletictrainersystem.com/CompanyHistory.aspx>

⁴ <https://www.athletictrainersystem.com/Default.aspx>

32. Upon information and belief, among the universities served by Keffer are Defendant University and Jane Doe 1's alma mater.

33. Keffer represents that its Athletic Trainer System tool was "designed with athletic trainers for athletic trainers," and is designed to store personal identifying information and personal health information belonging to students including their treatment histories, diagnoses, injuries, photos, and personal details, like height and weight, mental health information, and demographic information.⁵

34. In Keffer's FAQ, it boasts that: "Keffer Development hosts all databases in our SSAE-16, SOC II and FedRamp certified data center" and that "Information security is a high priority in our company."⁶ Keffer further claims that "On top of our Data Center being FedRamp Certified, ATS is also HIPAA and FERPA compliant. We utilize a company called Compliance Helper to ensure we maintain HIPAA and FERPA compliance."⁷

35. In Keffer's Privacy Policy, it acknowledges that it has obligations as a "business associate" under HIPAA: "To the extent that KDS [Keffer] receives or maintains patient medical information in the course of providing the Clinical EMR, that information is secured, used and disclosed only in accordance with KDS' legal obligations as a "business associate" under HIPAA."⁸

36. Keffer's Privacy Policy further states: "KDS understands that storing our data in a secure manner is essential. KDS stores PII, PHI and other data using industry-standard physical, technical and administrative safeguards to secure data against foreseeable risks, such as

⁵ See <https://www.athletictrainersystem.com/DemoRequest.aspx>

⁶ https://www.athletictrainersystem.com/pdf_Files/ATS_FAQ.pdf

⁷ *Id.*

⁸ https://www.athletictrainersystem.com/pdf_Files/ATS_Privacy_Policy.pdf

unauthorized use, access, disclosure, destruction or modification. Please note, however, that while KDS has endeavored to create a secure and reliable website for users, the confidentiality of any communication or material transmitted to/from the Website or via e-mail cannot be guaranteed.”⁹

37. Despite recognizing these obligations, Keffer failed to implement basic, industry standard systems to protect students’ – including Jane Doe 1’s personal identifying information and protected health information.

38. As an example, while Keffer maintained the option to incorporate two-factor authentication to access its Athletic Trainer System applications, it did not require that institutions and users do so.¹⁰ A two-factor basic security measure that requires an additional layer of authentication on top of a login credential, such as a code sent via text message or email – and critically, would have prevented Defendant Weiss from gaining access to student protected health information with only the access credentials belonging to other administrators and users.

39. Defendants knew that Keffer did not require institutions and users to use two-factor authorization to access the private information and communications accessible through its system, including information maintained in the Defendant Malone University’s facilities, and thus knowingly and deliberately permitted Plaintiff’s confidential information and communications to be accessed, shared, and divulged without authorization from Plaintiff.

40. Recent actions by the FTC underscore the gross negligence and failings of Keffer and Defendant Malone University in failing to ensure that the Athletic Trainer System was configured to default to two-factor or multi-factor authentication for access to its systems containing personal identifying information and protected health information. In February 2023,

⁹ *Id.*

¹⁰ https://www.athletictrainersystem.com/pdf_Files/ATS_FAQ.pdf

the FTC published an article titled, *Security Principles: Addressing Underlying Causes of Risk in Complex Systems*. The article highlighted the importance of multi-factor authentication (MFA), stating: “Multi-factor authentication is widely regarded as a critical security practice because it means a compromised password alone is not enough to take over someone’s account.”¹¹

41. Additionally, the FTC’s enforcement actions over the past five years further emphasize the critical and fundamental role MFA plays in an effective data security system, where the FTC has repeatedly obtained MFA as a form of injunctive relief in data security enforcement actions.¹²

42. Keffer also lacked any effective data auditing program to measure the download activity from its system, which would have allowed it to detect the massive, years-long data breach on its systems by Defendant Weiss and the resulting cyber sexual assault on Plaintiff Jane Doe 1 and those Class Members similarly situated.

43. Both Keffer and Defendant Malone University had a responsibility and duty to protect the private data of student athletes stored within their database and to have mechanisms in place to prevent such a gross invasion of privacy as what occurred in this case.

44. The risk of identity theft and breaches of security to access users’ private, personal, and confidential information is foreseeable within the University and Keffer’s information technology systems, and the University and Keffer are well aware of the foreseeable risks of

¹¹<https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems>

¹² E.g., *In re: Equifax* (July 2019), <https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach>; *In re Drizly* (Oct. 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million>.

breaches, such as those alleged in this case, that are likely to occur if their practices in detecting, preventing, and mitigating such breaches are substandard.

C. DEFENDANT UNIVERSITY’S FAILURE TO SAFEGUARD ITS STUDENTS’ PRIVATE INFORMATION FOR NEARLY A DECADE

45. Defendant Malone University is an established high-level educational institution, with a diverse athletic program, enrolling approximately 399 student athletes at any one time in 19 different sports at the NCAA Division 2 level.

46. In maintaining its athletics department and programs, Malone University provides its student athletes with athletic trainers.

47. The University had a responsibility and duty to oversee the University’s operations, policies and procedures, and to care for and protect the University’s students.

48. The University was required to ensure that students, such as Jane Doe 1, were not exposed to sexual predators who would invade their privacy.

49. The University failed in this duty by failing to take any reasonable action to prevent the harm caused to Jane Doe 1 and other Class Members as alleged in this Complaint.

50. This prolific and egregious breach and violation was entirely preventable by the University and Keffer. As noted in a criminal complaint filed by the U.S. Attorney for the Eastern District of Michigan, Defendant Weiss breached Keffer’s systems and the systems of colleges and universities across this nation by exploiting passwords and other vulnerabilities in the systems and authentication processes of Keffer and these universities. On information and belief, neither the University nor Keffer required that its employees or students implement safeguards like multi-factor authentication to access accounts, a standard practice for all entities collecting personal identifying information, especially medical data and PHI (protected health information).

51. The breach and cyber assaults were a direct result of Defendant Malone University's and Keffer's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Jane Doe 1 and Class Members PII and PHI, leaving the most sensitive and personal information of students, like Jane Doe 1, vulnerable to exploitation by malicious predators like Defendant Weiss.

52. Defendant Malone University was grossly negligent on two fronts: (1) in its hiring and oversight of Defendant Keffer and its entrusting of students' PII and PHI in the care of Defendant Keffer, and (2) in its maintenance, oversight and security of its own internal databases of those internal systems to protect student PII and PHI.

53. The University took no reasonable actions to prevent this access despite its duties to students and has taken no reasonable actions to notify or rectify harm to the victims of Matthew Weiss' misconduct and predation.

54. Thousands of students still remain at risk because the University and Keffer have failed to undertake any reasonable review of how Jane Doe 1's private and personal information is stored, maintained, and who can access such information, and from where.

55. To this day, the University has not formally informed Class Members impacted by Weiss' cyber sexual assault and misconduct.

D. MALONE UNIVERSITY WAS NEGLIGENT IN HIRING/CONTRACTING WITH DEFENDANT KEFFER AND IN ENTRUSTING STUDENTS PII AND PHI TO KEFFER

56. Defendant Malone University provided its student athletes medical treatment, including from athletic trainer employees of the University.

57. To facilitate that treatment, the University contracted with Keffer to use its Athletic Training System application, which required that student athletes provide the University and Keffer with sensitive PII and PHI.

58. When collecting that information, the University, like Keffer, accepted an obligation to protect that information under contract and statutory principles, including as a “business associate” under HIPAA.

59. Jane Doe 1 and others similar to her entrusted that the University and Keffer would safeguard her private information and ensure the security and confidentiality of her data.

60. The University and Keffer had, and continue to have, a duty to protect Jane Doe 1 and to take appropriate security measures to protect private, personal, medical and intimate information, communications, and images.

61. The University knowingly and deliberately permitted access to and divulging of Plaintiff’s stored communications through Keffer and failed to take reasonable action to ensure that Keffer protected the privacy of the sensitive information of Jane Doe 1 and others like her.

62. Upon information and belief, the University failed to properly investigate Keffer and Keffer’s protocols, and failed to adequately monitor or establish safeguards for Keffer’s work with the students and their private information to ensure they carried out their duties to safeguard and protect the private information of their students entrusted to them.

63. The University was negligent and/or reckless in failing to ensure that media and other private, personal and sensitive information, including but not limited to those of Jane Doe 1, was securely protected, as the University was entrusted to do.

64. The University failed to implement the security measures necessary to protect their students PII and PHI, including failing to train staff and employees on securing credentials,

requiring multi-or-two-factor authentication to use Keffer's Athletic Trainer System, overseeing third-party vendors like Keffer, in which the University entrusted students sensitive PII and PHI and monitoring and auditing access to student files and private information.

65. In other words, the University not only failed to ensure it had implemented sufficient security protocols and procedures across its own systems and staff, but also the University failed to ensure Keffer had adequate security measures in place to protect its students' PII and PHI from theft and misuse.

66. The University lacked adequate training programs to detect and stop breaches like those caused by Defendant Weiss.

67. The University and Keffer failed to implement reasonable protective measures to detect Weiss' irregular activity and trespassing, including but not limited to, appropriate authentication tools, behavioral analytics, anomaly detection, machine learning, and real-time monitoring of user activity, looking for deviations from established patterns and suspicious actions like unusual login attempts or access to sensitive data, any of which would have prevented Weiss' improper access to private student information.

68. Because Keffer and the University failed to implement basic, industry standard security measures, together these Defendants allowed an alleged sexual predator, ex-football coach Matthew Weiss, to access students', and in particular female student athletes', most sensitive information for nearly a decade.

69. All Defendants disregarded the rights of Jane Doe 1 and Class Members. The University and Keffer knowingly, intentionally, willfully, recklessly and/or negligently provided access to and/or divulged Plaintiff's private communications stored in their facilities; failed to take adequate and reasonable measures to ensure their data systems were protected against

unauthorized intrusions; failed to disclose that they did not have adequately robust computer systems and security practices to safeguard private information; failed to take standard and reasonably available steps to prevent the data breach and cyber assault; failed to properly train their staff and employees on proper security measures; failed to provide Jane Doe 1 and the Class Members prompt notice of the data breach and cyber assault.

70. Defendants Malone University's and Keffer's conduct amounts to a violation of the duties they owed to Jane Doe 1 under common law and state and federal statutory law, rendering them liable to Jane Doe 1 and the Class Members for the harms caused by this egregious and preventable cyber sexual assault and invasion of privacy. Defendant Weiss is equally liable for the harms inflicted on Jane Doe 1 and the Class Members by his intentional hacking and exfiltration of their private information under tort and statutory law.

71. Jane Doe 1 and the putative Class Members are current and former students at Malone University and other affected institutions in the United States that were specifically targeted by Weiss and harmed by the violation of their privacy.

72. Jane Doe 1 and the putative Class Members suffered injury as a result of Defendants' conduct. These injuries included: invasion and loss of privacy, loss of dignity, humiliation, embarrassment, and severe emotional distress.

73. Jane Doe 1 seeks to remedy these harms of behalf of herself and all similarly situated individuals whose private information was accessed by Weiss.

74. Jane Doe 1 seeks remedies including, but not limited to, compensatory damages, nominal damages, punitive damages, and reimbursement of out-of-pocket costs. Jane Doe 1 also seeks injunctive and equitable relief to prevent future injury on behalf of herself and the putative Class Members.

E. JANE DOE 1'S ALLEGATIONS

75. Plaintiff Jane Doe 1 is a former student athlete at Malone University.

76. While in school at Malone University, Jane Doe 1 participated in the swimming program while Defendant Weiss's data breach and cyber sexual assault was ongoing.

77. As a student athlete, Jane Doe 1 received treatment from the University's athletic trainer staff, requiring her to disclose information about her treatment, including height, weight, injuries, medications, treatment plans, and analysis on performance and recovery. To receive treatment, Jane Doe 1 was required to use the Keffer database, and the PII and PHI Jane Doe 1 disclosed was saved on the Keffer system.

78. As a student, Jane Doe 1 was required to disclose personal information to the University and was issued a University email where sensitive, personal information was stored.

79. Because Keffer and the University never implemented the security safeguards needed to protect Jane Doe 1's PII and PHI, Defendant Weiss compromised the PII and PHI belonging to every student whose information was saved by the University and/or Keffer's Athletic Trainer System database, including, on information and belief, Jane Doe 1's private and personal information.

80. Defendant Weiss compromised all information that was saved in the University and/or Athletic Trainer System databases, including Plaintiff's treatment information, injury information, height, weight, and other highly sensitive information.

81. Jane Doe 1 has received notice from the U.S. Department of Justice Victim Notification System that she was identified as a potential victim in the federal action against Defendant Weiss.¹³

82. After receiving notice from the federal government that read: “If you are receiving this notification, it means that information of yours was found in possession of the defendant,”¹⁴ Jane Doe 1 felt violated, deeply disturbed, humiliated, embarrassed, and extremely emotionally distressed; and is experiencing physical manifestations of the stress and anxiety caused by this egregious violation of her privacy – symptoms that are further exacerbated by the fact that Jane Doe 1 still does not have a full and complete understanding of the data breach and cyber sexual assault perpetrated by Defendant Weiss.

83. This cyber sexual assault invaded Plaintiff’s privacy and has devastated her personally and emotionally, as her highly sensitive private information was stolen by an alleged predator under circumstances that were entirely preventable by Defendant University and Defendant Keffer.

84. Upon information and belief, the United States Department of Justice is in the process of notifying thousands of potential victims that their privacy was breached.

85. As a direct result of the negligence, recklessness, and misconduct of the Defendants, Jane Doe 1 and those similarly situated have incurred substantial monetary and emotional damages exceeding \$5,000,000, exclusive of costs, interest, and fees.

¹³ See **Exhibit A**.

¹⁴ *Id.*

DEFENDANTS KEFFER AND MALONE UNIVERSITY
FAILED TO PROPERLY PROTECT PLAINTIFF'S AND CLASS
MEMBERS' PII AND PHI

86. Defendants Keffer and University did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted PII and PHI it was maintaining for Plaintiff and Class Members, causing the exposure of PII and PHI for 150,000 students and former students, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for approximately 3,330 students and former students.

87. The FTC promulgated numerous guides which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

88. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.¹⁵ The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.¹⁶

¹⁵ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

¹⁶ *Id.*

89. The FTC further recommends that companies not maintain PII and PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

90. Defendants Keffer and Malone University failed to properly implement basic data security practices explained and set forth by the FTC.

91. Defendants Keffer's and Malone University's failure to employ reasonable and appropriate measures to protect against unauthorized access PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

92. A systematic, years-long breach such as the ones Defendants Keffer and Malone University experienced is also considered a breach under the HIPAA Rules because there is an unauthorized access to PHI that is not permitted under HIPAA.

93. A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." 45 C.F.R. 164.40.

94. Data breaches are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the

covered entity or business associate must initiate its security incident and response and reporting procedures. 45 C.F.R.164.308(a)(6).¹⁷

95. Defendants Keffer's and Malone University's data breach was the foreseeable consequence of a combination of insufficiencies that demonstrate that Defendants Keffer and Malone University failed to comply with safeguards mandated by HIPAA.

**DEFENDANTS MALONE UNIVERSITY AND KEEFER
FAILED TO COMPLY WITH INDUSTRY STANDARDS**

96. Defendants Keffer and Malone University did not utilize industry standards appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of PII and PHI for approximately 150,000 students and former students, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for 3,330 students and former students.

97. As explained by the FBI, "[p]revention is the most effective defense against cyberattacks] and it is critical to take precautions for protection."¹⁸

98. To prevent and detect cyberattacks, including the cyberattack that resulted in this prolific data breach and cyber sexual assault, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of cyberattacks and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

¹⁷ *FACT SHEET: Ransomware and HIPPA*, U.S. Dept of Health and Hum. Servs., at 4 (July 11, 2016), <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>.

¹⁸ *See* How to Protect Your Networks from RANSOMWARE, at 3, <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Dec. 20, 2024).

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common cyberware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.¹⁹

¹⁹ *Id.* at 3-4.

99. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the data breach and cyber sexual assault, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the Internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . .
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it....
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic....²⁰

100. To prevent and detect cyberattacks, including the cyberattack that resulted in the data breaches and cyber sexual assaults, Defendants Keffer and Malone University could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure Internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection

²⁰ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), <https://www.cisa.gov/news-events/news/protecting-against-ransomware> (last visited Feb. 20, 2025).

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].²¹

101. As described above, experts studying cyber security routinely identify medical facilities as being particularly vulnerable to cyberattacks because of the value of the private information they collect and maintain.

102. Several best practices have been identified that at a minimum should be implemented by institutions such as Defendants Keffer and Malone University, including, but not limited to, the following: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

103. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

104. Given that Defendants Keffer and Malone University were storing the private information of 150,000 individuals combined, Defendants Keffer and Malone University could and should have implemented all of the above measures to prevent cyberattacks, along with the two-or multi-factor authentication discussed earlier in this Complaint.

²¹ See *Human-Operated Ransomware Attacks: A Preventable Disaster* (Mar 5, 2020), <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>.

105. The occurrence, scope and duration of the breach and cyber sexual assaults indicates that Defendants Keffer and Malone University failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the exposure of approximately 150,000 students' and former students' PII and PHI, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for 3,330 students and former students.

**DEFENDANTS KEFFER AND UNIVERSITY FAILED TO PROPERLY
PROTECT PII AND PHI**

106. Defendants Keffer and Malone University breached their obligations to Jane Doe 1 and Class Members and were otherwise grossly negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches, cyber-attacks, hacking incidents, and ransomware attacks;
- b. Failing to adequately protect students' private information;
- c. Failing to properly monitor its own data security systems for existing or prior intrusions;
- d. Failing to test and assess the adequacy of its data security system;
- e. Failing to develop adequate training programs related to the proper handling of emails and email security practices;
- f. Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;
- g. Failing to require a data security system to ensure the confidentiality and integrity of electronic PHI its network created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- h. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access to

only those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

- i. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);
- j. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);
- k. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- l. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- m. Failing to ensure that it was compliant with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);
- n. Failing to train all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);
- o. Failing to ensure that the electronic PHI it maintained is unusable, unreadable, or indecipherable to unauthorized individuals, as Defendants had not encrypted the electronic PHI as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” (45 C.F.R. §164.304 definition of encryption);
- p. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;
- q. Failing to adhere to industry standards for cybersecurity.

107. As the result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendants Keffer and Malone University negligently and unlawfully failed to safeguard Plaintiff’s and Class Members’ private, sensitive information.

108. Defendant Malone University was also grossly negligent in its failure to oversee the data security practices of third-party vendor—Keffer—in which it entrusted the sensitive private information of its students and former students.

109. Accordingly, as outlined below, Plaintiff and Class Members have already been severely harmed by this egregious violation of their privacy by Defendant Weiss.

CLASS ALLEGATIONS

110. Plaintiff files this lawsuit both individually and as representative of all others similarly situated pursuant to Fed. R. Civ. P. 23 on behalf of the following Class:

All students whose personal data, images, information, social media, or videos were accessed by Weiss without authorization (the “Class Members”).

111. In addition, Plaintiff believes a subclass may be appropriate for all class members who receive notice from the United States Department of Justice as to the likely violation of their privacy and rights by Weiss. Therefore, Plaintiff pleads a subclass as follows:

All students whose personal data, images, information, social media, or videos were accessed by Weiss without authorization and who received a notice letter from the United States Department of Justice as to Weiss (the “DOJ Letter Sub-Class”).

112. Excluded from the Class are: (a) Defendants and any entity or division in which Defendants have a controlling interest, and their legal representatives, officers, directors, assigns, and successors; (b) the Judge to whom this case is assigned and the Judge’s staff; and (c) the attorneys representing any parties to this Class Action.

113. Plaintiff reserves the right to modify or amend the definition of the proposed class and/or sub-classes before the Court determines whether certification is appropriate.

NUMEROSITY – FED. R. CIV. P. 23(A)(1)

114. Law enforcement officials have disclosed the numbers of victims is significant and exceeds one thousand satisfying the numerosity requirement. Although the exact number of Class Members is uncertain at this time, it will certainly be ascertained through appropriate discovery, the number is great enough such that joinder is impracticable.

115. The members of the Class are so numerous and geographically disperse that individual joinder of all members is impracticable.

116. Similarly, Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

117. Class Members are readily identifiable from information and records in the possession of the federal and state authorities, the University, and Keffer.

118. Electronic records maintained by the University and Keffer can confirm the identification of Class Members.

COMMONALITY AND PREDOMINANCE – FED. R. CIV. P. 23(A)(2) AND 23(B)(3)

119. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and the other Class Members. Similar or identical violations, practices, and injuries are involved, and the burden of proof to establish violations of those rights involve uniform, objective questions of fact and law, both for the prosecution and for the defense.

120. The common questions of fact and law existing as to all Class Members predominate over questions affecting only individual class members. The evidence required to advance Plaintiff's and Class Members' claims are the same, common to all; as is true of the

evidence Defendants will likely rely upon in defense of this action. Thus, the elements of commonality and predominance are both met.

121. For example, establishing the facts of how, where, who, when, and through what means the invasions of Plaintiff's and other Class Members occurred are identical.

122. Defendants' actions, inactions, negligence, and recklessness apply commonly to Plaintiff and Class Members.

123. The downloads and invasions by Weiss and the improper conduct accessing private information through unsecure facilities without permission is common to all Class Members and has caused injury to the Plaintiff and Class Members in common manners.

124. The majority of legal and factual issues of the Plaintiff and the Class Members predominate over any individual questions, including:

- (a) Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members private information;
- (b) Whether Defendants Keffer and the University failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the hacking incident and cyber sexual assault;
- (c) Whether Defendants Keffer and the University's data security systems prior to and during the data breach and cyber sexual assault complied with applicable data security laws and regulations;
- (d) Whether Defendants Keffer's and the University's data security systems prior to and during the data breach and cyber sexual assault were consistent with industry standards;
- (e) Whether Defendants Keffer and the University owed a duty to Plaintiff and Class Members to safeguard their private information;
- (f) Whether Defendants Keffer and the University breached their duty to Plaintiff and Class Members to safeguard their private information;
- (g) Whether Defendant University was grossly negligent and/or negligent in its oversight of Defendant Keffer;

- (h) Whether Defendant University or Keffer knew or should have known that their data security systems and monitoring processes were deficient;
- (i) Whether Defendants Keffer and the University owed a duty to provide Plaintiff and Class Members timely notice of the data breach and cyber sexual assaults, and whether Defendants Keffer and the University breached that duty to provide timely notice;
- (j) Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;
- (k) Whether Defendants' conduct was negligent or grossly negligent;
- (l) Whether Defendants' conduct was per se negligent;
- (m) Whether Defendants' conduct violated federal laws;
- (n) Whether Defendants' conduct violated state laws;
- (o) Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or punitive damages; and
- (p) Other common questions of fact and law relative to this case that remain to be discovered.

125. Resolving the claims of these Class Members in a single action will provide benefit to all parties and the Court by preserving resources, avoiding potentially inconsistent results, and providing a fair and efficient manner to adjudicate the claims.

126. Predominance does not require Plaintiff to prove an absence of individualized damage questions, or even proof of class wide damage in the aggregate. *Kuchar v. Saber Healthcare Holdings LLC*, 340 F.R.D. 115, 123 (N.D. Ohio 2021) (finding individualized damages questions also do not defeat a predominance finding and noting "when adjudication of questions of liability common to the class will achieve economies of time and expense, the predominance standard is generally satisfied even if damages are not provable in the aggregate.")(citing *Hicks*, 965 F.3d at 460).

TYPICALITY – FED. R. CIV. P. 23(A)(3)

127. Plaintiff’s claims are typical of those of other Class Members because all had their private information compromised as a result of the breach and cyber assault and Defendants’ malfeasance.

128. Plaintiff’s claims are typical of the Class Members because they are highly similar and the same and related in timing, circumstance, and harm suffered. To be sure, there are no defenses available to Defendants that are unique to individual Plaintiffs. The injury and causes of actions are common to the Class as all arising from the same statutory and privacy interests.

129. In *Halliburton Co. v. Erica P. John Fund, Inc.*, 573 U.S. 258, 276 (2014) the Supreme Court concluded that so long as plaintiffs could show that their evidence is capable of proving the key elements to plaintiffs’ claim on a class-wide basis, the fact that the defendants would have the opportunity at trial to rebut that presumption as to some of the plaintiffs did not raise individualized questions sufficient to defeat predominance. “That the defendant might attempt to pick off the occasional class member here or there through individualized rebuttal does not cause individual questions to predominate.” *Id.*

130. Certification of Plaintiff’s claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

131. The need to conduct additional post certification stage discovery, such as further file review or class member surveys, to eliminate uninjured persons after trial, does not act as a *de facto* bar to certification. *Nixon*, 2021 WL 4037824, at *8 (citing *Young*, 693 F.3d at 540); *In re Visa Check/MasterMoney Antitrust Litig.*, 280 F.3d 124, 145 (2d Cir. 2001); *Perez v. First Am. Title Ins. Co.*, 2009 WL 2486003, at *7 (D. Ariz. Aug. 12, 2009) (“Even if it takes a substantial

amount of time to review files and determine who is eligible for the [denied] discount, that work can be done through discovery.”); *Slapikas v. First Am. Title Ins. Co.*, 250 F.R.D. 232, 250 (W.D. Pa. 2008) (finding class action manageable despite First American's assertion that “no database exists easily and efficiently to make the determination that would be required for each file”).

132. Any remaining disputes on membership or class members damages can be left to a special master’s decision. *Whitlock v. FSL Mgmt., LLC*, 2012 WL 3274973, at *12 (W.D. Ky., 2012), *aff’d*, 843 F.3d 1084 (6th Cir. 2016). By placing the validation of injury step at the end of the class trial process, no injured class members are left out, and at the same time, Defendants are not at risk for paying any uninjured class members.

ADEQUACY OF REPRESENTATION – FED. R. CIV. P. 23(A)(4)

133. Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that she has no interests that are in conflict with those of the Class Members. In addition, she has retained counsel competent and experienced in complex class action litigation, and she will prosecute this action vigorously. The Class’s interests will be fairly and adequately protected by Plaintiff and her counsel.

SUPERIORITY OF CLASS TREATMENT – FED. R. CIV. P. 23(B)(3)

134. The class action is superior to any other available procedures for the fair and efficient adjudication of these claims, and no unusual difficulties are likely to be encountered in the management of this class action.

135. The superiority analysis required to certify a class is designed to achieve economies of time, effort and expense, and to promote uniformity of decisions as to persons similarly placed, without sacrificing procedural fairness or bringing about other undesirable results.

136. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable.

137. It would be an unnecessary burden upon the court system to require these individual Class Members to institute separate actions. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

138. Pursuing this matter as a class action is superior to individual actions because:

- (a) Separate actions by Class Members could lead to inconsistent or varying adjudications that would confront Defendants with potentially incompatible standards of conduct;
- (b) Many victims will not come forward without a certified class;
- (c) Final equitable relief will be appropriate with respect to the entire Class as a whole for monitoring, protection, therapy and other equitable forms of relief that may be provided;
- (d) This action is manageable as a class action and would be impractical to adjudicate any other way;
- (e) Absent the class action, individual Class Members may not know if their privacy was invaded; where such images are currently being stored, or are accessible by others; and their injuries are likely to go unaddressed and unremedied; and,
- (f) Individual Class members may not have the ability or incentive to pursue individual legal action on their own.

PARTICULAR ISSUES – FED. R. CIV. P. 23(C)(4)

139. In the event unforeseen issues preclude class certification under Fed.R.Civ.P. 23(b)(3), the case is still appropriate for class certification under Fed.R.Civ.P. 23(c)(4), as to the particular issues of liability.

140. Defendants have acted or refused to act on grounds generally applicable to Plaintiff and the other members of the Class, thereby making declaratory relief, as described below, with respect to the Class as a whole.

COUNT I
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT – 18 U.S.C. § 1030
(Against Defendant Weiss)

141. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

142. Plaintiff alleges that Defendant Weiss violated the Computer Fraud and Abuse Act.

143. Weiss violated the Computer Fraud and Abuse Act by unlawfully accessing Plaintiff's private information without authorization.

144. Weiss' actions constituted a violation of the Act because by entering the digital network and extracting sensitive private information of students, he "intentionally accesse[d] a computer without authorization" and/or "exceed[ed] authorized access, and thereby obtain[ed] ... information." 18 U.S.C. § 1030(a)(2)(C).

145. Weiss' actions were deliberate because he knew he was unauthorized and proceeded, nevertheless.

146. Under 18 U.S.C. § 1030(g), Plaintiff may recover damages in this civil action from Weiss along with injunctive relief or other equitable relief.

147. Given the willful violations committed by Weiss, resulting in significant damage, harm, humiliation, and distress to Plaintiff and other Class Members, Plaintiff should be awarded all appropriate damages in this matter.

COUNT II
VIOLATIONS OF THE STORED COMMUNICATIONS ACT
18 U.S.C. § 2701 et seq
(Against Defendants Weiss, Keffer, and University)

148. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

149. Plaintiff alleges that Defendants Weiss, Keffer, and University violated the Stored Communications Act.

150. The Stored Communications Act, 18 U.S.C. § 2701 et seq., prohibits the unauthorized access of web-based cloud storage and media accounts such as those at issue and other accounts hosted by Defendants University and Keffer that contain personal, private, and intimate information and communications about and relating to Plaintiff and others situated similarly to Plaintiff.

151. Specifically, under 18 U.S.C. § 2701(a), it is unlawful for any person to: (1) intentionally access without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceed an authorization to access that facility; and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system.

152. Under 18 U.S.C. § 2702, it is unlawful for a person or entity providing an electronic communication service to the public to knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service or to divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of a subscriber or customer of such service, solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the

contents of any such communications for purposes of providing any services other than storage or computer processing.

153. Plaintiff's electronic information and communications were in electronic storage and clearly fall within the scope of the statute.

154. Defendant Weiss was not authorized to access or divulge the content of Plaintiff's private communications by for any purpose.

155. The information, messages, files, and media were accessed by Weiss without authorization.

156. Weiss' access without authorization were deliberate.

157. There is no manner in which Plaintiff's private information, messages, files, and media could have been obtained without unauthorized access and would not have been obtained without unauthorized access had Defendants University and Keffer not knowingly divulged or permitted access to such information, through Keffer Development other channels, despite knowing that the information would not be protected.

158. Under Section 2707 of the Stored Communications Act, individuals may bring a civil action for the violation of this statute.

159. This law imposes strict liability on violators.

160. The statute provides that a person aggrieved by a violation of the act may seek appropriate relief including equitable and declaratory relief, actual damages or damages no less than \$1,000 punitive damages, and reasonable attorney's fee[s] and other litigation costs reasonably incurred according to 18 U.S.C. § 2707(b)-(c).

161. Defendants' access to and divulging of Plaintiff's private, personal, and intimate information, messages, files, and media constituted a violation of 18 U.S.C. §§ 2701 and 2702.

162. The University, Keffer, and Weiss knew they did not have authority to access and divulge Plaintiff's private, personal, and intimate information, messages, files, and media but did so anyway.

163. Defendants' knowing or intentional conduct led to multiple violations of the Stored Communications Act.

164. As a result of these violations, Plaintiff has incurred significant monetary and nonmonetary damages as a result of these violations of the Stored Communications Act, and Plaintiff seeks appropriate compensation for her damages.

165. Under the statute, Plaintiff should be granted the greater of (1) the sum of their actual damages suffered and any profits made by the University and Weiss as a result of the violations or (2) \$1,000 per violation of the Stored Communications Act.

166. Given these violations were deliberate, the Court should assess punitive damages against Defendants as well.

167. Plaintiff should also be granted reasonable attorney fees and costs.

**COUNT III – VIOLATION OF TITLE IX, 20 U.S.C. § 1681(A) Et Seq.
(Against Defendant Malone University)**

168. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

169. Plaintiff alleges that Defendant Malone University violated Title IX, 20 U.S.C. § 1681(A) et seq.

170. Defendant Malone University receives federal financial support for its educational programs and is therefore subject to the provisions of Title IX of the Education Act of 1972, 20 U.S.C. § 1681(a), et seq.

171. Title IX mandates that “No person in the United States shall on the basis of sex, be ... subject to discrimination under any education program or activity receiving Federal financial assistance ...”

172. Plaintiff and Class Member are “persons” under the Title IX statutory language.

173. Weiss specifically targeted women in his unwanted invasions of privacy and his misconduct is discrimination on the basis of sex.

174. Defendant Malone University, under Title IX, is obligated to investigate allegations of sexual harassment.

175. Defendant Malone University was aware of the sensitive nature of the private and personal information of Plaintiff to which Weiss was able to access.

176. Defendant Malone University acted with deliberate indifference to sexual harassment by:

- a. Failing to protect Plaintiff and others as required by Title IX;
- b. Neglecting to adequately investigate and address the complaints regarding the deeply sensitive information Plaintiff provided;
- c. Failing to institute corrective measures to prevent Weiss from sexually harassing students; and
- d. Failing to adequately investigate the other multiple acts of deliberate indifference.

177. Defendant Malone University acted with deliberate indifference as their lack of response to the sexual harassment was clearly unreasonable in light of the known circumstances.

178. Defendant Malone University’s failure to promptly and appropriately protect, investigate, and remedy and respond to the sexual harassment of women has effectively denied

them equal educational opportunities at the University, including access to medical care and sports training.

179. At the time the Plaintiff received some medical and/or athletic training services from the University, she did not know the Defendant failed to adequately consider her safety.

180. As a result of Defendant Malone University's deliberate indifference, Plaintiff has suffered loss of educational opportunities and/or benefits.

181. Plaintiff has incurred, and will continue to incur, attorney's fees and costs of litigation.

182. At the time of Defendants' misconduct and wrongful actions and inactions, Plaintiff was unaware, and or with reasonable diligence could not have been aware, of Defendants' institutional failings with respect to their responsibilities under Title IX.

183. Defendant Malone University maintained a policy and/or practice of deliberate indifference to protection of female student athletes.

184. Defendant's policy and/or practice of deliberate indifference to protection against the invasion of privacy for female athletes created an increased risk of sexual harassment.

185. Despite being able to prevent these privacy violations and acts of harassment, Defendant failed to do so.

186. Because of the Defendant Malone University's policy and/or practice of deliberate indifference, Plaintiff had her privacy invaded and was sexually harassed by Weiss.

187. Plaintiff should be awarded all such forms of damages in this case for Defendant Malone University's conduct that caused great damage, humiliation, and embarrassment to Plaintiff and the Class.

**COUNT IV - VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.
§ 1983 - UNREASONABLE SEARCH AND SEIZURE
(Against Defendant Weiss)**

188. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

189. Plaintiff alleges Defendant Weiss violated her civil rights under 42 U.S.C. § 1983 and the Fourth Amendment of the U.S. Constitution.

190. Defendant Weiss, sued in his individual capacity, was a state employee at all times relevant to this action, and acted under color of state law to deprive Plaintiff of her "rights, privileges or immunities secured by the Constitution and laws" of the United States, 42 U.S.C. § 1983, specifically their Fourth Amendment right to be free warrantless and unreasonable searches and seizures.

191. At the time of his actions giving rise to this case, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally searched and seized Plaintiff's private information without her consent, without a warrant, without probable cause or reasonable suspicion, and without any lawful basis or justification, in violation of Plaintiff's clearly established rights under the Fourth Amendment.

192. The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated "

193. It is well settled that the Fourth Amendment's protection extends beyond the sphere of criminal investigations. *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 755 (2010) (citing *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 530 (1967)).

194. "The [Fourth] Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government," without regard to whether the government actor is investigating crime or performing another function." *Id.* (quoting *Skinner v. Railway Labor Executives' Assn.*, 489 U.S. 602, 613-614 (1989)).

195. Plaintiff had a reasonable and legitimate expectation of privacy in her private, personal, and intimate information and images.

196. Acting under color of law, Defendant Weiss violated Plaintiff's clearly established right not to have their private, personal, and intimate information and images. accessed, searched, viewed, and seized when he searched and seized Plaintiff's private, personal, and intimate information and images without a warrant, without reasonable suspicion, without probable cause, and without any lawful basis, justification or need to support such an intrusion on Plaintiff's reasonable and legitimate expectation of privacy in that information.

197. Defendant Weiss' search and seizure of Plaintiff's personal information was per se unreasonable under the Fourth Amendment.

198. Defendant Weiss' search and seizure of Plaintiff's private, personal, and intimate information and images was unjustified at its inception and was not related in scope to any circumstances that would justify the search and seizure in the first place.

199. Defendant Weiss is not entitled to qualified immunity because Plaintiff's rights under the Fourth Amendment not to have their personal information searched and seized by him without a warrant, without permission, and without any lawful basis or justification, was obvious and clearly established when Weiss accessed Plaintiff's private information, such that no reasonable person in Weiss's position would believe that the act of searching and seizing Plaintiff's private information was lawful under the specific circumstances presented, and Weiss had fair warning

under the law as it existed at the time of his actions that those actions obviously violated Plaintiff's rights under the Fourth Amendment. See, e.g., *G.C. v. Owensboro Public Schools*, 711 F.3d 623 (6th Cir. 2013) (Holding that high school officials violated the Fourth Amendment by searching a student's cell phone and reading his text messages); see also *Brannum v. Overton County School Bd.*, 516 F.3d 489, 499 (Stating that "Some personal liberties are so fundamental to human dignity as to need no specific explication in our Constitution in order to ensure their protection against government invasion[.]" and holding that school officials violated Fourth Amendment by installing cameras to surreptitiously record students in locker rooms.)

200. As a direct and proximate result of Weiss' violation of Plaintiff's Fourth Amendment rights, Plaintiff has suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

201. Plaintiff should be awarded all such forms of damages in this case for Weiss' conduct that caused great damage, humiliation, and embarrassment to Plaintiff and the Class.

**COUNT V -- VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.
§ 1983 - DUE PROCESS/BODILY INTEGRITY
(Against Defendant Weiss)**

202. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

203. Plaintiff is alleging Defendant Weiss violated her civil rights under 42 U.S.C. § 1983 and the Fourteenth Amendment of the U.S. Constitution.

204. Defendant Weiss, sued in his individual capacity, was a state employee at all times relevant to this action, and acted under color of state law to deprive Plaintiff of her "rights, privileges or immunities secured by the Constitution and laws" of the United States, 42 U.S.C. § 1983, specifically their Fourteenth Amendment equal protection right to be free from sexual

harassment in an educational setting, and her Fourteenth Amendment due process right to be free from violation of bodily integrity. *West v. Atkins*, 487 U.S. 42, 49-50 (1988) (quoting *Lugar v. Edmondson Oil Co.*, 457 U.S. 922, 936 n. 18 (1982)).

205. At the time of the actions giving rise to this case, it was obvious, clearly established, and known to Weiss that the right to be free from sexual abuse at the hands of a state employee was protected by the Due Process Clause of the Fourteenth Amendment, such that he knew his actions in accessing Plaintiff's private, personal, and intimate information and images violated Plaintiff's fundamental right of due process. *Doe v. Claiborne Cnty., Tenn. By & Through Claiborne Cnty. Bd. of Educ.*, 103 F.3d 495, 506-07 (6th Cir. 1996) (Stating that "the Due Process Clause protects students against abusive governmental power as exercised by a school. To be sure, the magnitude of the liberty deprivation that sexual abuse inflicts upon the victim is an abuse of governmental power of the most fundamental sort; it is an unjustified intrusion that strips the very essence of personhood. If the "right to bodily integrity" means anything, it certainly encompasses the right not to be sexually assaulted under color of law. This conduct is so contrary to fundamental notions of liberty and so lacking of any redeeming social value, that no rational individual could believe that sexual abuse by a state actor is constitutionally permissible under the Due Process Clause.").

206. At the time of his actions giving rise to this case, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally engaged in actions which violated Plaintiff's right of bodily integrity, in violation of the Due Process Clause.

207. Weiss' actions were malicious, intentionally harmful, and were taken with deliberate indifference, and were so outrageous as to shock the contemporary conscience.

208. As a direct and proximate result of Weiss' violation of Plaintiff's Fourteenth Amendment rights, Plaintiff has suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

209. Plaintiff should be awarded all such forms of damages in this case for Weiss's conduct that caused great damage, humiliation, and embarrassment to Plaintiff and the Class.

**COUNT VI -- VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.
§ 1983 - EQUAL PROTECTION
(Against Defendant Weiss)**

210. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

211. Plaintiff is alleging Defendant Weiss violated their civil rights under 42 U.S.C. § 1983 and the Fourteenth Amendment of the U.S. Constitution.

212. Weiss' deliberate and intentional actions in accessing Plaintiff's personal, private, and intimate images and information constituted sexual harassment and abuse because Weiss accessed Plaintiff's highly sensitive, private, and personal information, data, and media for his own personal and sexual purposes.

213. At the time of the actions giving rise to this case, it was obvious, clearly established, and known to Weiss that the right to be free from gender discrimination, including sexual harassment and abuse at the hands of a state employee, was protected by the Equal Protection Clause of the Fourteenth Amendment, such that Weiss knew his actions in accessing Plaintiff's personal, private, and intimate images and information violated Plaintiff's rights under the Fourteenth Amendment. *Fitzgerald v. Barnstable Sch. Comm.*, 555 U.S. 246, 257-258 (2009); see also *Daniels v. Board of Education*, 805 F.2d 203, 206-07 (6th Cir.1986); *Gutzwiller v. Fenik*, 860

F.2d 1317, 1325 (6th Cir. 1988); *Kitchen v. Chippewa Valley Sch.*, 825 F.2d 1004, 1012 (6th Cir. 1987).

214. At the time of his actions giving rise to this case, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally engaged in sexual harassment and sexual abuse, in violation of the Equal Protection Clause.

215. As a direct and proximate result of Weiss' violation of Plaintiff's Fourteenth Amendment rights, Plaintiff has suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

216. Plaintiff should be awarded all such forms of damages in this case for Weiss' conduct that caused great damage, humiliation, and embarrassment to Plaintiff and the Class.

**COUNT VII -- VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.
§ 1983 - DUE PROCESS/DEPRIVATION OF PROPERTY
(Against Defendant Weiss)**

217. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

218. Plaintiff alleges that Defendant Weiss violated her civil rights under 42 U.S.C. § 1983 and the Fourteenth Amendment of the U.S. Constitution.

219. Defendant Weiss, sued in his individual capacity, was a state employee at all times relevant to this action, and acted under color of state law to deprive Plaintiff of her "rights, privileges or immunities secured by the Constitution and laws" of the United States, 42 U.S.C. § 1983, specifically her Fourteenth Amendment due process right to be free of deprivations of property without due process

220. At the time of the actions giving rise to this case, it was obvious, clearly established, and known to Weiss that the right not to be deprived of one's property without due process was protected by the Due Process Clause of the Fourteenth Amendment, such that he knew his actions in accessing and misappropriating Plaintiff's private, personal, and intimate information and images violated Plaintiff's fundamental right of due process.

221. Plaintiff and others similarly situated had a protected property interest in their personal, private, intimate, and confidential information.

222. At the time of his actions giving rise to this case, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally engaged in actions which violated Plaintiff's right not to be deprived of her personal property, in violation of the Due Process Clause.

223. Weiss' actions were malicious, intentionally harmful, and were taken with deliberate indifference, and were so outrageous as to shock the contemporary conscience.

224. As a direct and proximate result of Weiss' violation of Plaintiff's Fourteenth Amendment rights, Plaintiff has suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

225. Plaintiff should be awarded all such forms of damages in this case for Weiss' conduct that caused great damage, humiliation, and embarrassment to Plaintiff and the Class.

COUNT VIII – INVASION OF PRIVACY – INTRUSION UPON SECLUSION
(Against Defendants Weiss, Malone University, and Keffer)

226. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

227. Plaintiff alleges Defendant Weiss intentionally invaded Plaintiff's and Class Members' privacy by intruding upon their seclusion.

228. Plaintiff's and Class Members' PII/PHI, social media files, videos, and other images were each in electronic storage and were intended to be kept private.

229. Plaintiff and Class Members had a reasonable expectation of privacy in the PII/PHI, social media files, videos and other images Defendant Weiss hacked, accessed, viewed, exfiltrated, and kept detailed personal notes on.

230. Defendant Weiss unlawfully and intentionally engaged in the unwarranted appropriation and exploitation of Plaintiff's and Class Members' PII/PHI personality and publicized their private affairs that the public has no legitimate concern.

231. Defendant Weiss unlawfully and intentionally engaged in the wrongful intrusion into the Plaintiff's and Class Members' PII/PHI private activities in such a manner as to outrage and caused mental suffering, shame and humiliation to a person of ordinary sensibilities.

232. Defendant Weiss unlawfully and intentionally accessed this private and personal information, invading on the seclusion and private affairs of Plaintiff and Class Members.

233. Defendant Weiss' actions were unauthorized, wrongful, and the invasion would be highly offensive to any reasonable person.

234. Plaintiff never granted permission for this access and Defendant Weiss' intrusion is a severe violation of their privacy, causing them severe emotional damages.

235. This information would not have been obtained absent the negligence and misconduct of the Defendants.

236. Plaintiff feels embarrassed, ashamed, humiliated, and distressed that their private information has been accessed by strangers and third parties.

237. Defendant Weiss actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

238. Plaintiff alleges the University and Keffer are vicariously liable for Defendant Weiss invading Plaintiffs' and the Class Members' privacy by intruding upon their seclusion.

239. Plaintiff and Class Members are entitled to compensatory, consequential, punitive, and nominal damages suffered as a result of the extensive data breaches and cyber sexual assaults.

COUNT IX – GROSS NEGLIGENCE
(Against Defendants Malone University and Keffer)

240. Plaintiff restates and incorporate the allegations set forth above as if fully set forth herein.

241. Plaintiff alleges Defendants Malone University and Keffer were grossly negligent.

242. Plaintiff and Class members entrusted Keffer and the University to store, secure, and safeguard their PII/PHI, media, photos, videos and other personal data.

243. The University, Plaintiff, and Class Members entrusted Defendants to keep Plaintiff's and the Class Members' information private.

244. Plaintiff and the Class Members relied on Defendants to securely maintain their personal, private information and data.

245. Plaintiff and Class Members did not authorize access to such information, data, and media by Defendant Weiss.

246. Plaintiff and Class Members had the right to keep such information, data, and media private, and had a reasonable expectation that Defendants Malone University and Keffer would do so.

247. Defendants Malone University and Keffer had a duty to securely maintain the Plaintiff's and Class Members' PII/PHI and digital data.

248. Defendants Malone University and Keffer were grossly negligent and breached their duties owed to the Plaintiff and Class Members by:

- a. Failing to securely maintain their database to prevent unauthorized access of personal and private information;
- b. Failing to implement reasonable protective measures to detect Defendant Weiss' unauthorized access and irregular activity, including, but not limited to appropriate authentication tools, behavioral analytics, anomaly detection, machine learning, and real-time monitoring of user activity;
- c. Failing to appropriately monitor for deviations from expected patterns and suspicious logins, including multiple failed attempts to access accounts, unusual log-in attempts, or repeated access to sensitive data;
- d. Failing to notify the Plaintiff and Class Members that their personal, private data had been improperly accessed;
- e. Demonstrating a reckless disregard; and
- f. Other gross negligence to be discovered.

249. The Plaintiff's and Class Members PII and PHI, data, and media could not have been accessed but for Defendants' recklessness and indifference.

250. Had Defendants securely maintained Plaintiff's and Class Members' data, this would have prevented Defendant Weiss from improperly and unlawfully accessing the PII and PHI of Plaintiff's and the Class Members' and would have prevented even further invasions of their privacy, namely the accessing and collection of their personal, intimate images and videos.

251. It was foreseeable that the personal, sensitive information of young females, and female athletes may be a target of hacking, as such, reasonable care required Defendants Malone University and Keffer to have appropriate systems in place to prevent such hacking and alerting them to such activity so it could be immediately terminated and not allowed to persist and continue.

252. Defendants Malone University and Keffer were clearly aware of the potential risks and consciously decided to act in a manner that disregarded those risks to the Plaintiff and the Class Members.

253. Plaintiff and the Class Members are embarrassed, ashamed, humiliated, and mortified that their private information has been accessed by total strangers and third parties.

254. Defendants' failures and omissions to secure this private data was so reckless and indifferent that it shows a substantial lack of concern for injuries to Plaintiff and the Class Members.

255. Plaintiff and Class Members have incurred significant monetary and non-monetary damages as a result of Defendants' reckless and indifferent actions, and should be awarded damages accordingly.

COUNT X – NEGLIGENCE AND NEGLIGENCE PER SE
(Against Defendants Malone University and Keffer)

256. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

257. Plaintiff and Class Members entrusted their PII and PHI to Defendants Malone University and Keffer (collectively "Defendants" in this Count).

258. Defendants owed Plaintiff and Class Members a duty to exercise reasonable care in handling and using the PII and PHI in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

259. Plaintiff and Class Members entrusted their PII and PHI to Defendants on the premise and with the understanding that Defendants would safeguard their information for

purposes that would benefit Plaintiffs and Class Members and/or not disclose their PII and PHI to unauthorized third parties.

260. Defendants owed a duty of care to Plaintiff and Class Members because it was foreseeable that failure to adequately safeguard their PII and PHI in accordance with industry standards concerning data security would result in the compromise of that PII and PHI—as occurred in this case.

261. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiff’s and Class Members’ PII and PHI by misrepresenting their commitments to high standards of security in their public representations on their websites and information systems, when in reality their lack of security allowed Plaintiffs’ and Class Members’ PII and PHI to be accessed and exfiltrated by malicious actors including Defendant Weiss.

262. Defendants further breached its duty of care to Plaintiffs and Class Members by failing to properly supervise both the way the PII and PHI was stored, used, and exchanged, and those in its employ who were responsible for ensuring the reasonable and adequate security of that PII and PHI.

263. Defendants had full knowledge of the sensitive nature of the PII and PHI and the types of harm that Plaintiff and Class Members could and would suffer if the PII and PHI was wrongfully disclosed.

264. Defendants knowingly collected, came into possession of, and maintained Plaintiff’s and Class Members’ PII and PHI, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty included, among other things, designing, maintaining,

and testing Defendants' security protocols to ensure that the PII and PHI of Plaintiffs and Class Members in Defendants' possession was adequately secured and protected.

265. Defendants had, and continue to have, a duty to timely disclose that Plaintiff's and Class Members' PII and PHI within their possession was compromised and precisely the type(s) of information that were compromised.

266. Defendants had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII and PHI.

267. Defendants owed Plaintiff and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their PII and PHI. Defendants also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the breach/breaches.

268. Defendants owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Keffer knew or should have known would suffer injury-in-fact from Defendants' inadequate security protocols. Defendants actively sought and obtained Plaintiffs' and Class Members' PII and PHI.

269. The risk that unauthorized persons would attempt to gain access to the PII and PHI in Defendants' care, and misuse it was foreseeable. Given that Defendants hold vast amounts of PII and PHI, it was inevitable that unauthorized individuals would attempt to access the databases containing the PII and PHI.

270. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like HIPAA and/or Section 5 of the FTC Act, Ohio Rev. Code §§ 3798 *et seq.* and other

requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII/PHI.

271. These regulations were intended to protect the Plaintiff and Class Members at issue here, and Defendants' failure to abide by them caused Plaintiff and the Class Members damages.

272. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PHI is properly maintained.

273. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs and Class Members, which is recognized by laws and regulations, as well as common law. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class Members from a data breach and was considered a "business associate" under HIPAA.

274. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

275. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential PII and PHI.

276. Defendants systematically failed to provide adequate security for data in its possession.

277. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiff or Class Members.

278. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

- a. Upon information and belief, mishandling emails, so as to allow for unauthorized person(s) to access Plaintiffs' and Class Members' PII and PHI;
- b. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs', Class Members' PII and PHI, including, but not limited to, its failure to require two- or multi-factor authentication for access to its Athletic Trainer System;
- c. Failing to adequately monitor the security of its networks and systems;
- d. Failure to periodically ensure that their computer systems and networks had plans in place to maintain reasonable data security safeguards and detect an unauthorized access;
- e. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);
- f. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2)
- g. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- h. Failing to ensure compliance with HIPAA security standards under 45 C.F.R. § 164.306(a)(4);
- i. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- j. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1); and
- k. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security

incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

279. Defendants, through their actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs and Class Members' PII and PHI within Defendants' possession.

280. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' and Class Members' private, personal, information.

281. Defendants, through their actions and/or omissions, unlawfully breached their duty to timely disclose to Plaintiffs and Class Members that the PII and PHI within Defendants' possession might have been compromised and precisely the type of information compromised.

282. It was foreseeable that Defendants' failure to use reasonable measures to protect Plaintiffs and Class Members' PII and PHI would result in injury to Plaintiffs and Class Members.

283. It was foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' PII and PHI would result in injuries to Plaintiffs and Class Members.

284. Defendants' breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' PII and PHI to be compromised.

285. Defendants' failure to exercise reasonable care actually and proximately caused Plaintiffs and Class Members actual, tangible, injury-in-fact and damages, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

286. Plaintiffs are embarrassed, ashamed, humiliated, and mortified that their private information has been accessed by total strangers and third parties.

287. Defendants' failures and omissions to secure this private data was so negligent that it shows a substantial lack of concern for injuries to Plaintiffs and the Class Members.

288. Plaintiffs and those similarly situated have incurred significant monetary and nonmonetary damages as a result of Defendants' actions, and should be awarded damages accordingly.

XI – BREACH OF IMPLIED CONTRACT
(Against Defendant Keffer)

289. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

290. Defendant Keffer, as a condition of providing its services, required Plaintiff and Class Members to provide and entrust their PII and PHI.

291. By Plaintiff and Class Members providing their PII and PHI to Defendant Keffer, and by Defendant Keffer accepting this PII and PHI and representing it would maintain the safety and security of this PII and PHI, including through its privacy policies, the parties mutually assented to implied contracts. These implied contracts included an implicit agreement and understanding that (1) Defendant Keffer would adequately safeguard Plaintiff's and Class Members' PII and PHI from foreseeable threats, (2) that Defendant Keffer would delete the information of Plaintiff and Class Members once it no longer had a legitimate need; and (3) that Defendant Keffer would provide Plaintiff and Class Members with notice within a reasonable amount of time after suffering a data breach.

292. Defendant Keffer provided consideration by providing its services, while Plaintiff and Class Members provided consideration by paying for its services, either directly or indirectly through their enrollment at educational institutions, and providing valuable property – i.e., their PII and PHI – to Defendant Keffer. Defendant Keffer benefited from the receipt of this PII and PHI by increased income through providing its Athletic Trainer Software.

293. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant Keffer.

294. Defendant Keffer breached its implied contracts with Plaintiff and Class Members by failing to safeguard and protect their PII and PHI or providing timely and accurate notice to them that their PII and PHI was compromised due to the breaches and cyber assaults.

295. Defendant Keffer's breaches actually and proximately caused Plaintiff and Class Members actual, tangible, damages, which damages are ongoing, imminent, immediate and which they continue to face.

COUNT XII – UNJUST ENRICHMENT
(Against Defendant Keffer)

296. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

297. Plaintiff plead this Count in the alternative to their Implied Contract claim.

298. Plaintiff and Class Members conferred a monetary benefit on Defendant Keffer, either directly or indirectly through their educational institutions, by providing Defendant with payment for its services and with valuable PII and PHI in exchange for the use of Defendant Keffer's Athletic Trainer System software.

299. Defendant Keffer enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII and PHI.

300. Instead of providing a reasonable level of security that would have prevented the pervasive data breaches and cyber sexual assaults, Defendant Keffer instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper,

ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant Keffer's failure to provide the requisite security.

301. Under the principles of equity and good conscience, Defendant Keffer should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class Members, because Defendant Keffer failed to implement appropriate data management and security measures that are mandated by industry standards.

302. Defendant Keffer acquired the monetary benefit and PII and PHI through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

303. If Plaintiffs and Class Members knew that Defendant Keffer had not secured their PII and PHI, they would not have consented to provide it to Defendant Keffer, either directly or indirectly.

304. Plaintiff and Class Members have no adequate remedy at law.

305. Defendant Keffer actually and proximately caused Plaintiffs and Class Members actual, tangible, damages, which damages are ongoing, imminent, immediate, and which they continue to face.

306. As a direct and proximate result of Defendant Keffer's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

307. Defendant Keffer should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

COUNT XIII – TRESPASS TO CHATTELS
(Against Defendant Weiss)

308. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

309. Plaintiff alleges Defendant Weiss is guilty of trespass to chattels.

310. Plaintiff alleges the University and Keffer are vicariously liable for Defendant Weiss' trespass to chattels.

311. Defendant Weiss intentionally and unlawfully accessed Plaintiff's and Class Members' private and personal data, information, and media, thereby wrongfully asserting control over and interfering with their sensitive data without authorization.

312. This unauthorized access and control was deliberate and carried out with malicious intent.

313. Plaintiff and the Class Members have incurred significant monetary and nonmonetary damages as a result of Defendant Weiss' intentional misconduct.

314. Plaintiff and the Class Members are entitled to exemplary damages as a result of these intentional and harmful act and interference with, and wrongful exercise of control over, their property.

COUNT XIV – ASSAULT
(Against Defendants Weiss, Malone University, and Keffer)

315. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

316. Plaintiff alleges Defendant Weiss assaulted Plaintiff and Class Members.

317. Plaintiff alleges the University and Keffer are vicariously liable for Defendant Weiss' assault on Plaintiff and Class Members.

318. Defendant Weiss' conduct, in accessing Plaintiff's and other Class Members' personal and private information as outlined above was intentional without consent, authorization, or any legal justification.

319. Defendant Weiss' accessing Plaintiff's and other Class Members' personal and private information as outlined above had the apparent ability to cause harm.

320. Defendant Weiss' conduct caused a reasonable apprehension of imminent harm onto Plaintiff and Class Members.

321. As a result, Plaintiff and Class Members suffered severe damages and seek compensation as appropriate for these damages.

COUNT XV – INTENTIONAL INFLICTION OF EMOTIONAL DISTRESS
(Against Defendant Weiss)

322. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

323. Plaintiff alleges Defendant Weiss is guilty of intentional infliction of emotional distress on Plaintiff and Class Members.

324. Plaintiff alleges the University and Keffer are vicariously liable for Defendant Weiss' intentional infliction of emotional distress on Plaintiffs and Class Members.

325. Defendant Weiss' conduct in accessing Plaintiff's and Class Members' private and personal data, media, and information, as outlined above, was intentional or Defendant knew or should have known .

326. Defendant Weiss' conduct was both extreme and outrageous.

327. Defendant Weiss' access of Plaintiff's' and Class Members' private and personal data, information, and media was not for any proper or authorized use.

328. Defendant Weiss’ conduct caused severe emotional distress to Plaintiff and Class Members.

329. Plaintiff and Class Members suffered severe emotional distress and economic damage as a result of Weiss’ intentional actions and as such Plaintiffs seek compensation as appropriate for these damages.

**COUNT XVI – VIOLATION OF OHIO IDENTITY FRAUD AND PRIVATE DISCLOSURE
OF SECURITY BREACH OF COMPUTERIZED PERSONAL INFORMATION DATA
STATUTES**

**Ohio Revised Codes §§ 1349.19 and 2913.49
(*Against Defendants Weiss and Keffer*)**

330. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

331. Plaintiff alleges Defendants Weiss and Keffer violated Ohio’s Identity Fraud and Private Disclosure of Security Breach of Computerized Personal Information Data Statutes (collectively the “Ohio Identity Protection Statutes”) , Ohio Revised Codes §§ 1349.19 and 2913.49.

332. Plaintiff’s and Class Members personal and private media, content, data, and information were stored electronically and intended to be kept private.

333. Defendant Keffer is a “Business Entity” as that term is defined by the Ohio Identity Protection Statutes.

334. Defendant Keffer’s Athletic Trainer System software is a “System” as that term is defined by the Ohio Identity Protection Statutes.

335. Defendant Weiss unlawfully accessed Defendant Keffer’s System which contained Plaintiff’s and Class Members’ this private and personal information, data, and media without the

Plaintiff's and Class Members' express or implied consent, was not a good faith acquisition, nor accessed for any other lawful reason.

336. Defendant Weiss unlawfully accessing Defendant Keffer's System was a "Breach of the security of the system" as defined by the Ohio Identity Protection Statutes.

337. Defendant Weiss' actions were not authorized.

338. Defendant Keffer maintained a database of Plaintiffs' and Class Members' sensitive, personal information and protected health information.

339. Defendant Keffer had a duty to notify Plaintiffs and Class Members of the unauthorized breach of their very private data.

340. Defendants failed to notify Plaintiff and Class Members of such.

341. As a result, Plaintiff and Class Members were unaware for years that their very sensitive data was being accessed without their permission or authorization in violation of the Ohio Identity Protection Statutes.

342. As a result of Defendants' conduct, Plaintiff and Class Members suffered significant and severe damages and as such Plaintiffs seek compensation as appropriate for these damages.

COUNT XVII – CIVIL PENALTIES FOR CRIMINAL ACTS
Ohio Revised Codes § 2307.60
(Against Defendants Weiss, Keffer, and University)

343. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

344. Plaintiff alleges that Defendants Weiss, Keffer, and University violated the Stored Communications Act.

345. Plaintiff and Class Members assert this claim because the Defendants, separately and jointly violated:

- i. 18 U.S.C. § 1030 *et seq.*;
- ii. 18 U.S.C. § 2701 *et seq.*;
- iii. Title IX, 20 U.S.C. § 1681(A) *et seq.*;
- iv. 42 U.S.C. § 1983 *et seq.*;
- v. the Fourth Amendment of the U.S. Constitution;
- vi. the Fourteenth Amendment of the U.S. Constitution;
- vii. Ohio Revised Code § 2917.211;
- viii. Ohio Revised Codes § 1349.19; and,
- ix. Ohio Revised Codes § 2913.49

346. These statutes impose criminal penalties for violations.

347. By their acts and omissions described herein, Defendants have willfully violated these federal and Ohio statutes causing Plaintiff and Class Members injury.

348. O.R.C. § 2307.60 permits anyone injured in one person or property by a criminal act to recover damages in a civil action, including exemplary and punitive damages.

349. As a result of Defendants' willful violations of the statutes listed above, Plaintiff and Class members are entitled to compensatory and punitive damages pursuant to O.R.C. § 2307.60.

RELIEF

WHEREFORE, Plaintiff prays this Court grant the following relief:

- a. Enter a judgment encompassing the relief requested above, plus significant compensatory damages exceeding \$5,000,000.00 together with costs, interest and attorney fees, against Defendants, and such other relief to which they are entitled;

- b. An order certifying the proposed Class and Subclasses; designating Plaintiff as the named representative of the respective Class Members; and appointing her counsel as Class Counsel;
- c. All such equitable relief as the Court deems proper and just, including but not limited to, declaratory relief;
- d. An order finding that Defendants violated Ohio Rev. Code §§ 1349.19 and 2913.49;
- e. Award Plaintiff costs, attorney fees as well as interest from the date of Judgment until paid;
- f. Compensatory and punitive damages under O.R.C. § 2307.60
- g. Grant such further relief as is agreeable to equity and good conscience.

JURY DEMAND

For all triable issues, a jury is hereby demanded.

Dated: April 24, 2025

Respectfully submitted,

BARKAN MEIZLISH DEROSE COX, LLP

/s/ Robert E. DeRose

Robert E. DeRose (OH Bar No. 0055214)

Anna R. Caplan (OH Bar No. 0104562)

4200 Regent Street, Suite 210

Columbus, OH 43219

Phone: (614) 221-4221

Facsimile: (614) 744-2300

Email: bderose@barkanmeizlish.com

acaplan@barkanmeizlish.com

SOMMERS SCHWARTZ, P.C.

Lisa M. Esser (P70628) (*pro hoc vice anticipated*)

Richard L. Groffsky (P32992) (*pro hoc vice anticipated*)

Jason J. Thompson (P47184) (*pro hoc vice anticipated*)

Matthew G. Curtis (P37999) (*pro hoc vice anticipated*)

One Towne Square, 17th Floor

Southfield, MI 48076

Phone: (248) 355-0300

Email: LEsser@sommerspc.com

rgroffsky@sommerspc.com

JThompson@sommerspc.com

MCurtis@sommerspc.com

PITT MCGEHEE PALMER BONANNI & RIVERS, P.C.
Megan Bonanni (P52079) (*pro hoc vice anticipated*)
Kevin M. Carlson (P67704) (*pro hoc vice anticipated*)
Beth M. Rivers (P33614) (*pro hoc vice anticipated*)
Danielle Y. Canepa (P82237) (*pro hoc vice anticipated*)
117 W. Fourth Street, Suite 200
Royal Oak, MI 48067
Phone: (248) 398-9800
Email: mbonnani@pittlawpc.com
kcarlson@pittlawpc.com
brivers@pittlawpc.com
dcanepa@pittlawpc.com

Attorneys for Plaintiffs.

Exhibit A



17

3 Messages



DE-3728795 - Court Case 25-CR-20165

DO NOT REPLY TO THIS EMAIL.



March 31, 2025

U.S. Department of Justice

Eastern District of Michigan

Suite 2001

211 W. Fort St.

Detroit, MI 48226-3211

Phone: 1-844-527-5299

Email:

USAEO.MCAP@usdoj.gov

Re: United States v. Defendant(s) Matthew Weiss

Case Number 2023R00208 and Court Docket Number 25-CR-20165

Dear [REDACTED]:

This notice is provided by the United States Department of Justice Victim Notification System. I am contacting you because you were identified by law enforcement as a victim or potential victim during the investigation of the above criminal case.



CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

Jane Doe 1, individually and on behalf of all individuals similarly situated

(b) County of Residence of First Listed Plaintiff Cuyahoga
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

Robert E. DeRose (0055214), Anna R. Caplan
(0104562) Barkan Meizlish DeRose Cox, LLP, 4200
Regent St Ste 210 Columbus OH 43219

DEFENDANTS

Matthew Weiss, Malone University, and Keffer Development, LLC

County of Residence of First Listed Defendant _____

(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff
☒ 3 Federal Question (U.S. Government Not a Party)
☐ 2 U.S. Government Defendant
☐ 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- | | PTF | DEF | | PTF | DEF |
|---|----------------------------|----------------------------|---|----------------------------|----------------------------|
| Citizen of This State | <input type="checkbox"/> 1 | <input type="checkbox"/> 1 | Incorporated or Principal Place of Business In This State | <input type="checkbox"/> 4 | <input type="checkbox"/> 4 |
| Citizen of Another State | <input type="checkbox"/> 2 | <input type="checkbox"/> 2 | Incorporated and Principal Place of Business In Another State | <input type="checkbox"/> 5 | <input type="checkbox"/> 5 |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3 | <input type="checkbox"/> 3 | Foreign Nation | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 |

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Click here for: [Nature of Suit Code Descriptions.](#)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES	
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input checked="" type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice	PERSONAL INJURY <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act IMMIGRATION <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 INTELLECTUAL PROPERTY RIGHTS <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 835 Patent - Abbreviated New Drug Application <input type="checkbox"/> 840 Trademark <input type="checkbox"/> 880 Defend Trade Secrets Act of 2016 SOCIAL SECURITY <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit (15 USC 1681 or 1692) <input type="checkbox"/> 485 Telephone Consumer Protection Act <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
REAL PROPERTY <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	CIVIL RIGHTS <input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education	PRISONER PETITIONS Habeas Corpus: <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty Other: <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN (Place an "X" in One Box Only)

- ☒ 1 Original Proceeding
☐ 2 Removed from State Court
☐ 3 Remanded from Appellate Court
☐ 4 Reinstated or Reopened
☐ 5 Transferred from Another District (specify)
☐ 6 Multidistrict Litigation - Transfer
☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):

28 U.S.C. §1331 federal question 18 U.S.C. § 1030 et seq., 18 U.S.C. § 2701 et seq., Title IX, 20 U.S.C. § 1681(A) et seq., 42 U.S.C. § 1983 et seq.,

Brief description of cause:

Complaint for damages

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND \$

In excess \$5,000,000.0

CHECK YES only if demanded in complaint:

JURY DEMAND:

☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE

DOCKET NUMBER

DATE

SIGNATURE OF ATTORNEY OF RECORD

4/24/2025

/s/ Robert E. DeRose

FOR OFFICE USE ONLY

RECEIPT #

AMOUNT

APPLYING IFP

JUDGE

MAG. JUDGE

UNITED STATES DISTRICT COURT NORTHERN DISTRICT OF OHIO

I. Civil Categories: (Please check one category only).

1. ☒ General Civil
 2. ☐ Administrative Review/Social Security
 3. ☐ Habeas Corpus Death Penalty

*If under Title 28, §2255, name the SENTENCING JUDGE: _____

CASE NUMBER: _____

II. **RELATED OR REFILED CASES** See LR 3.1 which provides in pertinent part: "If an action is filed or removed to this Court and assigned to a District Judge after which it is discontinued, dismissed or remanded to a State court, and subsequently refiled, it shall be assigned to the same Judge who received the initial case assignment without regard for the place of holding court in which the case was refiled. Counsel or a party without counsel shall be responsible for bringing such cases to the attention of the Court by responding to the questions included on the Civil Cover Sheet."

This action: ☐ is **RELATED** to another **PENDING** civil case ☐ is a **REFILED** case ☐ was **PREVIOUSLY REMANDED**

If applicable, please indicate on page 1 in section VIII, the name of the Judge and case number.

III. In accordance with Local Civil Rule 3.8, actions involving counties in the Eastern Division shall be filed at any of the divisional offices therein. Actions involving counties in the Western Division shall be filed at the Toledo office. For the purpose of determining the proper division, and for statistical reasons, the following information is requested.

ANSWER ONE PARAGRAPH ONLY. ANSWER PARAGRAPHS 1 THRU 3 IN ORDER. UPON FINDING WHICH PARAGRAPH APPLIES TO YOUR CASE, ANSWER IT AND STOP.

(1) **Resident defendant** If the defendant resides in a county within this district, please set forth the name of such county

COUNTY:

Corporation For the purpose of answering the above, a corporation is deemed to be a resident of that county in which it has its principal place of business in that district.

(2) **Non-Resident defendant** If no defendant is a resident of a county in this district, please set forth the county wherein the cause of action arose or the event complained of occurred.

COUNTY:

(3) **Other Cases** If no defendant is a resident of this district, or if the defendant is a corporation not having a principle place of business within the district, and the cause of action arose or the event complained of occurred outside this district, please set forth the county of the plaintiff's residence.

COUNTY:

IV. The Counties in the Northern District of Ohio are divided into divisions as shown below. After the county is determined in Section III, please check the appropriate division.

EASTERN DIVISION

☐
☒
☐

AKRON

CLEVELAND

YOUNGSTOWN

(Counties: Carroll, Holmes, Portage, Stark, Summit, Tuscarawas and Wayne)
 (Counties: Ashland, Ashtabula, Crawford, Cuyahoga, Geauga, Lake, Lorain, Medina and Richland)
 (Counties: Columbiana, Mahoning and Trumbull)

WESTERN DIVISION

☐

TOLEDO

(Counties: Allen, Auglaize, Defiance, Erie, Fulton, Hancock, Hardin, Henry, Huron, Lucas, Marion, Mercer, Ottawa, Paulding, Putnam, Sandusky, Seneca VanWert, Williams, Wood and Wyandot)

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I.(a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
 - (b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
 - (c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
- United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here. United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
- Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
- Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).
- V. Origin.** Place an "X" in one of the seven boxes.
- Original Proceedings. (1) Cases which originate in the United States district courts.
- Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
- Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
- Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
- Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
- Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
- Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
- PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7.** Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.
- VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
- Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
- Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

ACCO,(MBKx),DISCOVERY,MANADR

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA (Eastern Division - Riverside)
CIVIL DOCKET FOR CASE #: 5:25-cv-00997-HDV-MBK**

Jane Doe 1 v. Matthew Weiss et al
Assigned to: Judge Hernan D. Vera
Referred to: Magistrate Judge Michael B. Kaufman
Demand: \$5,000,000
Cause: 28:1332 Diversity-Personal Injury

Date Filed: 04/23/2025
Jury Demand: Plaintiff
Nature of Suit: 360 P.I.: Other
Jurisdiction: Diversity

Plaintiff

Jane Doe 1
*individually and
on behalf of*
All others Similarly Situated

represented by **Yana A. Hart**
Clarkson Law Firm PC
22525 Pacific Coast Highway
Malibu, CA 90265
213-788-4050
Fax: 213-788-4070
Email: yhart@clarksonlawfirm.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Bryan Paul Thompson
Clarkson Law Firm, P.C.
22525 Pacific Coast Highway
Malibu, CA 90265
312-267-0061
Fax: 213-788-4070
Email: bthompson@clarksonlawfirm.com
ATTORNEY TO BE NOTICED

Jason J. Thompson
Sommers Schwatz PC
One Towne Square 17th Floor
Southfield, MI 48076
248-355-0300
Fax: 248-746-4001
Email: jthompson@sommerspc.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

Megan A Bonanni
Pitt McGehee Palmer Bonanni and Rivers
P.C.
117 W. Fourth Street Suite 200
Royal Oak, MI 48067
248-398-9800
Fax: 248-268-7996
Email: mbonanni@pittlawpc.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

Ryan J. Clarkson

Clarkson Law Firm PC
22525 Pacific Coast Highway
Malibu, CA 90265
213-788-4050
Fax: 213-788-4070
Email: rclarkson@clarksonlawfirm.com
ATTORNEY TO BE NOTICED

V.

Defendant**Matthew Weiss****Defendant****The Board of Trustees of the California
State University**

represented by **Amy Thomas Brantly**
Kesselman Brantly Stockinger LLP
1230 Rosecrans Avenue Suite 400
Manhattan Beach, CA 90266
310-307-4555
Fax: 310-307-4570
Email: Abrantly@kbslaw.com
ATTORNEY TO BE NOTICED

David W. Kesselman

Kesselman Brantly Stockinger LLP
1230 Rosecrans Avenue Suite 400
Manhattan Beach, CA 90266
310-307-4555
Fax: 310-307-4570
Email: dkesselman@kbslaw.com
ATTORNEY TO BE NOTICED

Mark Paluch

Kesselman Brantly Stockinger LLP
1230 Rosecrans Ave., Suite 400
Manhattan Beach, CA 90266
310-307-4555
Fax: 310-307-4570
Email: mpaluch@kbslaw.com
ATTORNEY TO BE NOTICED

Defendant**California State University San
Bernardino**

represented by **Amy Thomas Brantly**
(See above for address)
ATTORNEY TO BE NOTICED

David W. Kesselman

(See above for address)
ATTORNEY TO BE NOTICED

Mark Paluch

(See above for address)

*ATTORNEY TO BE NOTICED***Defendant****Keffer Development Services LLC**

represented by **Kyle Stephen Uhlman**
 Dillon McCandless King Coulter &
 Graham, LLP
 128 W. Cunningham Street
 Butler, PA 16001
 415-535-4117
 Email: kuhlman@dmkcg.com
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
04/23/2025	1	COMPLAINT Receipt No: ACACDC-39567126 - Fee: \$405, filed by Plaintiff Doe 1 Jane. (Attorney Yana A. Hart added to party Doe 1 Jane(pty:pla))(Hart, Yana) (Entered: 04/23/2025)
04/23/2025	2	Request for Clerk to Issue Summons on Complaint (Attorney Civil Case Opening) 1 filed by Plaintiff Doe 1 Jane. (Hart, Yana) (Entered: 04/23/2025)
04/23/2025	3	CIVIL COVER SHEET filed by Plaintiff Doe 1 Jane. (Hart, Yana) (Entered: 04/23/2025)
04/23/2025	4	NOTICE of Interested Parties filed by Plaintiff Doe 1 Jane, (Hart, Yana) (Entered: 04/23/2025)
04/28/2025	5	NOTICE OF ASSIGNMENT to District Judge Hernan D. Vera and Magistrate Judge Michael B. Kaufman. (sh) (Entered: 04/28/2025)
04/28/2025	6	NOTICE TO PARTIES OF COURT-DIRECTED ADR PROGRAM filed. (sh) (Entered: 04/28/2025)
04/28/2025	7	Notice to Counsel Re Consent to Proceed Before a United States Magistrate Judge. (sh) (Entered: 04/28/2025)
04/28/2025	8	21 DAY Summons Issued re Complaint (Attorney Civil Case Opening) 1 as to Defendants California State University San Bernardino, Keffer Development Services LLC, The Board of Trustees of the California State University, Matthew Weiss. (sh) (Entered: 04/28/2025)
04/28/2025	9	NOTICE OF PRO HAC VICE APPLICATION DUE for Non-Resident Attorney Megan Bonanni. A document recently filed in this case lists you as an out-of-state attorney of record. However, the Court has not been able to locate any record that you are admitted to the Bar of this Court, and you have not filed an application to appear Pro Hac Vice in this case. Accordingly, within 5 business days of the date of this notice, you must either (1) have your local counsel file an application to appear Pro Hac Vice (Form G-64) and pay the applicable fee, or (2) complete the next section of this form and return it to the court at cacd_attyadm@cacd.uscourts.gov . You have been removed as counsel of record from the docket in this case, and you will not be added back to the docket until your Pro Hac Vice status has been resolved. (sh) (Entered: 04/28/2025)
04/28/2025	10	NOTICE OF PRO HAC VICE APPLICATION DUE for Non-Resident Attorney Kevin M. Carlson. A document recently filed in this case lists you as an out-of-state attorney of record. However, the Court has not been able to locate any record that you are admitted to the Bar of this Court, and you have not filed an application to appear Pro Hac Vice in this case. Accordingly, within 5 business days of the date of this notice, you must either (1) have your local counsel file an application to appear Pro Hac Vice (Form G-64) and pay

		the applicable fee, or (2) complete the next section of this form and return it to the court at cacd_attyadm@cacd.uscourts.gov . You have been removed as counsel of record from the docket in this case, and you will not be added back to the docket until your Pro Hac Vice status has been resolved. (sh) (Entered: 04/28/2025)
04/28/2025	<u>11</u>	NOTICE OF PRO HAC VICE APPLICATION DUE for Non-Resident Attorney Lisa M. Esser. A document recently filed in this case lists you as an out-of-state attorney of record. However, the Court has not been able to locate any record that you are admitted to the Bar of this Court, and you have not filed an application to appear Pro Hac Vice in this case. Accordingly, within 5 business days of the date of this notice, you must either (1) have your local counsel file an application to appear Pro Hac Vice (Form G-64) and pay the applicable fee, or (2) complete the next section of this form and return it to the court at cacd_attyadm@cacd.uscourts.gov . You have been removed as counsel of record from the docket in this case, and you will not be added back to the docket until your Pro Hac Vice status has been resolved. (sh) (Entered: 04/28/2025)
04/28/2025	<u>12</u>	NOTICE OF PRO HAC VICE APPLICATION DUE for Non-Resident Attorney Jason Thompson. A document recently filed in this case lists you as an out-of-state attorney of record. However, the Court has not been able to locate any record that you are admitted to the Bar of this Court, and you have not filed an application to appear Pro Hac Vice in this case. Accordingly, within 5 business days of the date of this notice, you must either (1) have your local counsel file an application to appear Pro Hac Vice (Form G-64) and pay the applicable fee, or (2) complete the next section of this form and return it to the court at cacd_attyadm@cacd.uscourts.gov . You have been removed as counsel of record from the docket in this case, and you will not be added back to the docket until your Pro Hac Vice status has been resolved. (sh) (Entered: 04/28/2025)
04/28/2025	<u>13</u>	NOTICE OF PRO HAC VICE APPLICATION DUE for Non-Resident Attorney Richard L. Groffsky. A document recently filed in this case lists you as an out-of-state attorney of record. However, the Court has not been able to locate any record that you are admitted to the Bar of this Court, and you have not filed an application to appear Pro Hac Vice in this case. Accordingly, within 5 business days of the date of this notice, you must either (1) have your local counsel file an application to appear Pro Hac Vice (Form G-64) and pay the applicable fee, or (2) complete the next section of this form and return it to the court at cacd_attyadm@cacd.uscourts.gov . You have been removed as counsel of record from the docket in this case, and you will not be added back to the docket until your Pro Hac Vice status has been resolved. (sh) (Entered: 04/28/2025)
04/28/2025	<u>14</u>	NOTICE OF PRO HAC VICE APPLICATION DUE for Non-Resident Attorney Matthew G. Curtis. A document recently filed in this case lists you as an out-of-state attorney of record. However, the Court has not been able to locate any record that you are admitted to the Bar of this Court, and you have not filed an application to appear Pro Hac Vice in this case. Accordingly, within 5 business days of the date of this notice, you must either (1) have your local counsel file an application to appear Pro Hac Vice (Form G-64) and pay the applicable fee, or (2) complete the next section of this form and return it to the court at cacd_attyadm@cacd.uscourts.gov . You have been removed as counsel of record from the docket in this case, and you will not be added back to the docket until your Pro Hac Vice status has been resolved. (sh) (Entered: 04/28/2025)
04/29/2025	<u>15</u>	APPLICATION of Non-Resident Attorney Megan A. Bonanni to Appear Pro Hac Vice on behalf of Plaintiff Jane Doe 1 (Pro Hac Vice Fee - \$500 Fee Paid, Receipt No. ACACDC-39601420) filed by Plaintiff Jane Doe 1. (Attachments: # <u>1</u> Proposed Order Granting Pro Hac Vice Application of Megan A. Bonanni) (Hart, Yana) (Entered: 04/29/2025)
04/30/2025	<u>16</u>	APPLICATION of Non-Resident Attorney Jason J. Thompson to Appear Pro Hac Vice on behalf of Plaintiff Jane Doe 1 (Pro Hac Vice Fee - \$500 Previously Paid on 4/30/2025,

		Receipt No. ACACDC-39613981) filed by Plaintiff Jane Doe 1. (Attachments: # 1 Proposed Order Granting Pro Hac Vice Application of Jason J. Thompson) (Hart, Yana) (Entered: 04/30/2025)
05/02/2025	17	WAIVER OF SERVICE Returned Executed filed by Plaintiff Jane Doe 1. upon Keffer Development Services LLC waiver sent by Plaintiff on 5/2/2025, answer due 7/1/2025. Waiver of Service signed by Thomas W. King, III. (Hart, Yana) (Entered: 05/02/2025)
05/02/2025	18	NOTICE OF MOTION AND MOTION for Appointment of Counsel filed by Plaintiff Jane Doe 1. Motion set for hearing on 6/5/2025 at 10:00 AM before Judge Hernan D. Vera. (Attachments: # 1 Memorandum of Points and Authorities in Support of Motion for Appointment of Interim Lead Counsel, # 2 Declaration of Yana Hart, # 3 Exhibit 1, # 4 Exhibit 2, # 5 Exhibit 3, # 6 Exhibit 4, # 7 Exhibit 5, # 8 Exhibit 6, # 9 Exhibit 7, # 10 Exhibit 8, # 11 Exhibit 9, # 12 Exhibit 10, # 13 Exhibit 11, # 14 Exhibit 12, # 15 Proposed Order Granting Motion for Appointment of Interim Lead Counsel) (Hart, Yana) (Entered: 05/02/2025)
05/05/2025	19	ORDER by Judge Hernan D. Vera: granting 15 Non-Resident Attorney Megan A. Bonanni APPLICATION to Appear Pro Hac Vice on behalf of plaintiff Jane Doe 1, designating Yana Hart as local counsel. THERE IS NO PDF DOCUMENT ASSOCIATED WITH THIS ENTRY (ak) (Entered: 05/05/2025)
05/05/2025	20	ORDER by Judge Hernan D. Vera: granting 16 Non-Resident Attorney Jason J. Thompson APPLICATION to Appear Pro Hac Vice on behalf of plaintiff Jane Doe 1, designating Yana Hart as local counsel. THERE IS NO PDF DOCUMENT ASSOCIATED WITH THIS ENTRY (ak) (Entered: 05/05/2025)
05/05/2025	21	CIVIL STANDING ORDER by Judge Hernan D. Vera. (wm) (Entered: 05/05/2025)
05/28/2025	22	Notice of Appearance or Withdrawal of Counsel: for attorney David W. Kesselman counsel for Defendants California State University San Bernardino, The Board of Trustees of the California State University. Adding David W. Kesselman as counsel of record for Board of Trustees of the California State University, and California State University, San Bernardino for the reason indicated in the G-123 Notice. Filed by Defendant Board of Trustees of the California State University, and California State University, San Bernardino. (Attorney David W. Kesselman added to party California State University San Bernardino(pty:dft), Attorney David W. Kesselman added to party The Board of Trustees of the California State University(pty:dft))(Kesselman, David) (Entered: 05/28/2025)
05/28/2025	23	Notice of Appearance or Withdrawal of Counsel: for attorney Amy Thomas Brantly counsel for Defendants California State University San Bernardino, The Board of Trustees of the California State University. Adding Amy T. Brantly as counsel of record for Board of Trustees of the California State University, and California State University, San Bernardino for the reason indicated in the G-123 Notice. Filed by Defendants Board of Trustees of the California State University, and California State University, San Bernardino. (Attorney Amy Thomas Brantly added to party California State University San Bernardino(pty:dft), Attorney Amy Thomas Brantly added to party The Board of Trustees of the California State University(pty:dft))(Brantly, Amy) (Entered: 05/28/2025)
05/28/2025	24	Notice of Appearance or Withdrawal of Counsel: for attorney Mark Paluch counsel for Defendants California State University San Bernardino, The Board of Trustees of the California State University. Adding Mark Paluch as counsel of record for Board of Trustees of the California State University, and California State University, San Bernardino for the reason indicated in the G-123 Notice. Filed by Defendants Board of Trustees of the California State University, and California State University, San Bernardino. (Attorney Mark Paluch added to party California State University San Bernardino(pty:dft), Attorney

		Mark Paluch added to party The Board of Trustees of the California State University(pty:dft))(Paluch, Mark) (Entered: 05/28/2025)
05/28/2025	25	CSU DEFENDANTS RESPONSE TO PLAINTIFFS MOTION FOR APPOINTMENT OF INTERIM LEAD COUNSEL re NOTICE OF MOTION AND MOTION for Appointment of Counsel 18 filed by Defendants California State University San Bernardino, The Board of Trustees of the California State University. (Kesselman, David) (Entered: 05/28/2025)
05/30/2025	26	STIPULATION Extending Time to Answer the complaint as to California State University San Bernardino answer now due 7/9/2025; The Board of Trustees of the California State University answer now due 7/9/2025, re Complaint (Attorney Civil Case Opening) 1 filed by Board of Trustees of the California State University, and California State University, San Bernardino California State University San Bernardino; The Board of Trustees of the California State University.(Kesselman, David) (Entered: 05/30/2025)
05/30/2025	27	TEXT ONLY ENTRY (IN CHAMBERS) ORDER by Judge Hernan D. Vera: Pursuant to Rule 78 of the Federal Rules of Civil Procedure and Local Rule 7-15, the Court finds PLAINTIFF AND THE PROPOSED CLASS' MOTION FOR APPOINTMENT OF INTERIM LEAD COUNSEL 18 appropriate for decision without oral argument. The hearing set for 06/05/25 is hereby vacated and the matter taken off calendar. The matter will be deemed submitted on the vacated hearing date. THERE IS NO PDF DOCUMENT ASSOCIATED WITH THIS ENTRY. (wm) TEXT ONLY ENTRY (Entered: 05/30/2025)
06/05/2025	28	NOTICE of Appearance filed by attorney Kyle Stephen Uhlman on behalf of Defendant Keffer Development Services LLC (Attorney Kyle Stephen Uhlman added to party Keffer Development Services LLC (pty:dft))(Uhlman, Kyle) (Entered: 06/05/2025)

PACER Service Center			
Transaction Receipt			
06/05/2025 13:19:10			
PACER Login:	ThomaKingking	Client Code:	
Description:	Docket Report	Search Criteria:	5:25-cv-00997-HDV-MBK End date: 6/5/2025
Billable Pages:	6	Cost:	0.60

CLARKSON LAW FIRM, P.C.
Ryan J. Clarkson (SBN 257074)
rclarkson@clarksonlawfirm.com
Yana Hart (SBN 306499)
yhart@clarksonlawfirm.com
Bryan P. Thompson (SBN 354683)
bthompson@clarksonlawfirm.com
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050

**PITT MCGEHEE PALMER
BONANNI & RIVERS, P.C.**
Megan Bonanni*
mbonnani@pittlawpc.com
Kevin M. Carlson*
kcarlson@pittlawpc.com
117 W. Fourth Street, Suite 200
Royal Oak, MI 48067
Tel: (248) 398-9800

Counsel for Plaintiff and the Proposed Class

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA**

JANE DOE 1, individually and on
behalf of all others similarly situated,

Plaintiff,

vs.

MATTHEW WEISS, CALIFORNIA
STATE UNIVERSITY, SAN
BERNARDINO, BOARD OF
TRUSTEES OF THE CALIFORNIA
STATE UNIVERSITY, and KEFFER
DEVELOPMENT SERVICES, LLC,

Defendants.

SOMMERS SCHWARTZ, P.C.
Lisa M. Esser*
lessers@sommerspc.com
Jason Thompson*
jthompson@sommerspc.com
Richard L. Groffsky*
rgroffsky@sommerspc.com
Matthew G. Curtis*
mcurtis@sommerspc.com
One Towne Square, 17th Floor
Southfield, MI 48076
Tel: (248) 355-0300

** denotes PHV forthcoming*

Case No.: 5:25-cv-00997

CLASS ACTION COMPLAINT

JURY TRIAL DEMAND

**ACTION SEEKING STATEWIDE
AND NATIONWIDE RELIEF**

Plaintiff JANE DOE 1, (“Plaintiff”) through her attorneys, Sommers Schwartz, P.C., Pitt McGehee Palmer Bonanni & Rivers, P.C., and Clarkson Law Firm, P.C. for their Complaint against Matthew Weiss, California State University, San Bernardino, and Keffer Development Services, LLC, (“Defendants”) states as follows:

I. INTRODUCTION

1. Students and alumni connected to California State University, San Bernardino from 2015 to 2023—many of them student-athletes—have been subjected to a deeply troubling and unlawful breach of privacy, stemming from the actions of former University of Michigan and Baltimore Ravens coach Matthew Weiss, whose gross and despicable violations of their privacy were facilitated by institutional negligence. This class action lawsuit, filed against Matthew Weiss, California State University, San Bernardino and Keffer Development Services, LLC, seeks justice for the unauthorized access and misuse of personal information—an abuse so severe that California State University, San Bernardino students and student-athletes are now receiving formal notification from the U.S. Department of Justice that their private information, including intimate photos and videos, have been exposed, including Plaintiff Jane Doe 1. This action is brought to hold the Defendants accountable for failing to protect their students from foreseeable harm.

II. PARTIES

Plaintiff:

2. **Plaintiff Jane Doe 1** was a student athlete at California State University, San Bernardino between 2012-2016 and was a member of the Volleyball Team.

3. Plaintiff Jane Doe 1 is domiciled in Orange County, California, in the City of Huntington Beach.

4. On or about March 31, 2025, Plaintiff Jane Doe 1 received notice from the United States Department of Justice Victim Notification System that she was identified as a victim in the criminal case against University of Michigan’s Coach Weiss: *United States v. Defendant(s) Matthew Weiss*.

Defendants:

5. **California State University, San Bernardino** (“University”) is a public university in San Bernardino, State of California, San Bernardino County and is organized and existing under the laws of the State of California. Its principal place of business is in San Bernadino County.

6. University is a part of the California State University system.

7. **The Board of Trustees of the California State University** (“Trustees”) oversees the California State University system and is headquartered in Long Beach, California, and The Trustees are therefore sued as a Defendant in this action. (Collectively with California State University, San Bernardino the “University Defendants”)

8. **Defendant Keffer Development Services, LLC** (“Keffer”) is a Pennsylvania limited liability company in Grove City, PA, that has continuously and systemically conducted business in California by directly providing services to residents and entities within the State of California, thereby availing itself of protections of the law of the State of California.

9. Defendant Keffer is a technology and data vendor operating an electronic medical record and student athlete training system, which stored the personal identifying information (“PII”) and personal health information (“PHI”) of Plaintiff and Class Members across the country.

10. Any wrongful conduct and legal violations committed by Defendant Keffer that are subsequently outlined in this Complaint occurred specifically with respect to the Plaintiff during the time of the incident alleged in this Complaint.

11. **Matthew Weiss** (“Weiss”) is an individual residing in the State of Michigan, who had contacts with the State of California in that he conducted illegally activity in the State of California, by hacking into the personal property of Plaintiff and putative Class Members of the State of California during the applicable time

1 period at issue in this Complaint and said activities of which this Complaint arises
2 from.

3 12. On March 20, 2025, Defendant Weiss was indicted on 24 counts of
4 unauthorized access to computers and aggravated identity theft by the U.S. Attorney
5 for the Eastern District of Michigan.

6 **III. JURISDICTION AND VENUE**

7 13. Jurisdiction is proper in this Court under 28 U.S.C. §§ 1331 and 1367 as
8 this matter involves a claim under the Stored Communications Act, 18 U.S.C. §
9 2701(a) *et seq.*; the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; Title IX, 20
10 U.S.C. § 1681(A) *et seq.*; 42 U.S.C. § 1983; the Fourth Amendment of the U.S.
11 Constitution; and the Fourteenth Amendment of the U.S. Constitution, and this Court
12 has supplemental jurisdiction of all additional causes of action alleged in this
13 Complaint pursuant to 28 U.S.C. §1367(a).

14 14. This Court also has subject matter jurisdiction pursuant to 28 U.S.C.
15 §1332(d) under the Class Action Fairness Act (“CAFA”) as a class action lawsuit in
16 which the amount in controversy exceeds \$5,000,000.00, there are more than one-
17 hundred putative Class Members, and a number of the putative Class Members are
18 citizens of a state different than the state of which Defendants are citizens.

19 15. The Court has personal jurisdiction over Defendants named in this action
20 because University Defendants and Trustees are located and created under the laws
21 of the State of California, Defendant Weiss had minimum contacts with the State of
22 California as set forth above, thus purposefully availing himself of the privilege of
23 conducting activities in the State of California. Defendant Keffer directs business at
24 the State of California, conducts substantial business in California, and has availed
25 itself of the protections of California state law. The conduct by Defendant Keffer
26 which gives rise to the claims against Defendant Keffer in this Complaint was
27 directed at and occurred in the State of California.
28

17. Plaintiff's injuries are redressable by monetary compensation and injunctive relief, and all alleged injuries of Plaintiff and Class Members can be traced to Defendants' conduct.

Weiss' Data Breach and Cyber Sexual Assault of Thousands of Students for Nearly a Decade and the Role Defendant Keffer and University Defendants Played in his Scheme

19. Between 2015 and January 2023, Defendant Weiss gained unauthorized access to both student databases and student-athlete databases of more than 100 colleges and universities, some of which were maintained by Defendant Keffer, a third-party vendor contracted by these colleges and universities.

21. Due to lack of adequate security measures, failure to monitor their networks, databases, and accounts, Defendants enabled Weiss to gain access to Keffer's and University Defendants' databases, and download highly sensitive PII and PHI of more than 150,000 athletes – including Plaintiff's.

22. Using the information that Weiss obtained from the student-athlete databases, Weiss was then able to obtain access to the social media, email, and/or cloud storage accounts of more than 2,000 students. Defendant Weiss also illegally

1 obtained access to the social media, email, and/or cloud storage accounts of more than
2 1,300 additional students and/or alumni from universities and colleges across the
3 country. Once Weiss obtained access to these accounts, he downloaded personal,
4 intimate digital photographs and videos that were never intended to be shared beyond
5 intimate partners.

6 23. Defendant Weiss primarily targeted female college athletes. He
7 researched and targeted these women based on their school affiliation, athletic
8 history, and physical characteristics.

9 24. Through this scheme, unknown to students and student athletes,
10 Defendant Weiss downloaded intimate digital photographs and videos of female and
11 male students, and obtained highly sensitive private messages and information about
12 them. Plaintiff was one of these affected students.

13 25. This scheme appears to be the largest cyber sexual assault of student
14 athletes in U.S. history.

15 26. The data breach and cyber sexual assault of over 150,000 students from
16 university and college databases, including athletic databases maintained by Keffer,
17 and the targeted exfiltration of intimate, personal, digital photographs and videos of
18 3,300 students and athletes, continued for nearly a decade because the University
19 Defendants and Defendant Keffer failed to prevent, detect, or stop Weiss from
20 accessing those databases without and in excess of any authorization.

21 27. In at least several instances, Defendant Weiss exploited vulnerabilities in
22 universities' account authorization processes to gain access to the accounts of
23 students or alumni. Weiss then leveraged his access to these accounts to gain access
24 to other social media, email, and/or cloud storage accounts.

25 28. That level of access through that number of accounts is an egregious and
26 grossly negligent failure of data security, as no institution with reasonable data
27 security would allow such a breach over an eight-year period.
28

29. In March 2025, Matthew Weiss was charged in a 24-count indictment alleging 14 counts of unauthorized access to computers and 10 counts of aggravated identity theft, by the U.S. Attorney for the Eastern District of Michigan, for Weiss’ perpetration of the cyber sexual assaults and data breach.

Defendant Keffer and its “Athletic Trainer System”

30. Defendant Keffer is a software development vendor that developed an electronic medical record system known as “The Athletic Trainer System,” which is used by many schools, colleges, and universities across the United States.¹

31. Defendant Keffer was founded in 1994 and currently collaborates with over 600 clients across 48 states and internationally.² Defendant Keffer advertises that it currently serves over 6,500 schools, clinics, and other organizations with over 27,000 users and 2 million athletes.³

32. Upon information and belief, among the universities served by Keffer are Defendant University, Jane Doe 1’s alma mater.

33. Keffer represents that its Athletic Trainer System tool was “designed with athletic trainers for athletic trainers,” and is designed to store personal identifying information and personal health information belonging to students including their treatment histories, diagnoses, injuries, photos, and personal details, like height and weight, mental health information, and demographic information.⁴

¹ *ATS—Athlete Info*, THE ATHLETIC TRAINER SYSTEM, https://www.athletictrainersystem.com/pdf_files/Athlete_Info.pdf (last accessed April 22, 2025).

² *Company History*, THE ATHLETIC TRAINER SYSTEM, <https://www.athletictrainersystem.com/CompanyHistory.aspx> (last accessed April 22, 2025).

³ *The Athletic Trainer System*, THE ATHLETIC TRAINER SYSTEM, <https://www.athletictrainersystem.com/Default.aspx> (last accessed April 22, 2025).

⁴ *See Demo Request or Web Meeting Registration*, THE ATHLETIC TRAINER SYSTEM, <https://www.athletictrainersystem.com/DemoRequest.aspx> (last accessed April 22, 2025).

34. In Keffer’s FAQ, it boasts that: “Keffer Development hosts all databases in our SSAE-16, SOC II and FedRamp certified data center” and that “Information security is a high priority in our company.”⁵ Keffer further claims that “On top of our Data Center being FedRamp Certified, ATS is also HIPAA and FERPA compliant. We utilize a company called Compliance Helper to ensure we maintain HIPAA and FERPA compliance.”⁶

35. In Keffer’s Privacy Policy, it acknowledges that it has obligations as a “business associate” under HIPAA: “To the extent that KDS [Keffer] receives or maintains patient medical information in the course of providing the Clinical EMR, that information is secured, used and disclosed only in accordance with KDS’ legal obligations as a “business associate” under HIPAA.”⁷

36. Keffer’s Privacy Policy further states: “KDS understands that storing our data in a secure manner is essential. KDS stores PII, PHI and other data using industry-standard physical, technical and administrative safeguards to secure data against foreseeable risks, such as unauthorized use, access, disclosure, destruction or modification. Please note, however, that while KDS has endeavored to create a secure and reliable website for users, the confidentiality of any communication or material transmitted to/from the Website or via e-mail cannot be guaranteed.”⁸

37. Despite recognizing these obligations, Keffer failed to implement basic, industry standard systems to protect students’ – including Jane Doe 1’s personal identifying information and protected health information.

⁵ *The Athletic Trainer System FAQ*, THE ATHLETIC TRAINER SYSTEM, https://www.athletictrainersystem.com/pdf_Files/ATS_FAQ.pdf (last accessed April 22, 2025).

⁶ *Id.*

⁷ *Keffer Development Services, LLC Privacy Policy*, THE ATHLETIC TRAINER SYSTEM (July 2, 2024), https://www.athletictrainersystem.com/pdf_Files/ATS_Privacy_Policy.pdf (last accessed April 22, 2025).

⁸ *Id.*

38. As an example, while Keffer maintained the option to incorporate two-factor authentication to access its Athletic Trainer System applications, it did not require that institutions and users do so.⁹ A two-factor basic security measure, which requires an additional layer of authentication on top of a login credential – such as a code sent via text message or email – would have critically prevented Defendant Weiss from gaining access to student protected health information with only the access credentials belonging to other administrators and users.

39. Defendants knew that Keffer did not require institutions and users to use two-factor authorization to access the private information and communications accessible through its system, including information maintained in the Defendant University’s facilities, and thus knowingly and deliberately permitted Plaintiff’s confidential information and communications to be accessed, shared, and divulged without authorization from Plaintiff.

40. Recent actions by the FTC underscore the gross negligence and failings of Keffer and the University Defendants in failing to ensure that the Athletic Trainer System was configured to default to two-factor or multi-factor authentication for access to its systems containing personal identifying information and protected health information. In February 2023, the FTC published an article titled, *Security Principles: Addressing Underlying Causes of Risk in Complex Systems*. The article highlighted the importance of multi-factor authentication (MFA), stating: “Multi-factor authentication is widely regarded as a critical security practice because it means a compromised password alone is not enough to take over someone’s account.”¹⁰

⁹ *The Athletic Trainer System FAQ*, THE ATHLETIC TRAINER SYSTEM, https://www.athletictrainersystem.com/pdf_Files/ATS_FAQ.pdf (last accessed April 22, 2025).

¹⁰ Alex Gaynor, *Security Principles: Addressing underlying causes of risk in complex systems*, FEDERAL TRADE COMMISSION (Feb. 1, 2023), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems> (last accessed April 22, 2025).

41. Additionally, the FTC’s enforcement actions over the past five years further emphasize the critical and fundamental role MFA plays in an effective data security system, where the FTC has repeatedly obtained MFA as a form of injunctive relief in data security enforcement actions.¹¹

42. Keffer and the University Defendants also lacked any effective data auditing program to measure the download activity from its system, which would have allowed it to detect the massive, years-long data breach on its systems by Defendant Weiss and the resulting cyber sexual assault on Plaintiff Jane Doe 1 and those Class Members similarly situated.

43. Both Keffer and the University Defendants had a responsibility and duty to protect the private data of student athletes stored within their database and to have mechanisms in place to prevent such a gross invasion of privacy as what occurred in this case.

44. The risk of identity theft and breaches of security to access users’ private, personal, and confidential information is foreseeable within the University Defendants’ and Keffer’s information technology systems, and the University Defendants and Keffer are well aware of the foreseeable risks of breaches, such as those alleged in this case, that are likely to occur if their practices in detecting, preventing, and mitigating such breaches are substandard.

///

¹¹ E.g., *In re: Equifax* (July 2019), *Equifax to Pay \$575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach*, FEDERAL TRADE COMMISSION (July 22, 2019), <https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach> (last accessed April 22, 2025). ; *In re Drizly* (Oct. 2022), *FTC Takes Action Against Drizly and its CEO James Cory Rellas for Security Failures that Exposed Data of 2.5 Million Consumers*, FEDERAL TRADE COMMISSION (Oct. 24, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million> (last accessed April 22, 2025).

University Defendants’ Failure to Safeguard its Students’ Private Information for Nearly a Decade

45. California State University-San Bernardino is a high-level educational institution, with a diverse athletic program, enrolling hundreds of student athletes at any one time across over a dozen sports.

46. In maintaining its highly regarded athletics department and programs, California State University-San Bernardino provides its student athletes with athletic trainers.

47. The University Defendants had a responsibility and duty to oversee the University’s operations, policies, and procedures, and care for and protect the University’s students.

48. The University Defendants were required to ensure that students, such as Jane Doe 1, were not exposed to sexual predators who would invade their privacy.

49. The University Defendants failed in this duty by failing to take any reasonable action to prevent the harm caused to Jane Doe 1 and other Class Members as alleged in this Complaint.

50. This prolific and egregious breach and violation was entirely preventable by the University Defendants and Keffer. As noted in a criminal complaint filed by the U.S. Attorney for the Eastern District of Michigan, Defendant Weiss breached Keffer’s and the systems of colleges and universities across this nation by exploiting passwords and other vulnerabilities in the systems of Keffer and these universities and colleges and authentication processes. On information and belief, neither the University Defendants nor Keffer required that their employees or students implement safeguards like multi-factor authentication to access accounts, a standard practice for all entities collecting personal identifying information, especially medical data and PHI (“Protected Health Information”).

51. The breach and cyber assaults were a direct result of the University’s and Keffer’s failure to implement adequate and reasonable cyber-security procedures and

1 protocols necessary to protect Jane Doe 1 and Class Members PII and PHI, leaving
2 the most sensitive and personal information of students, like Jane Doe 1, vulnerable
3 to exploitation by malicious predators like Defendant Weiss.

4 52. The University Defendants were grossly negligent on two fronts: (1) in
5 their hiring and oversight of Defendant Keffer and their entrusting of students' PII
6 and PHI in the care of Defendant Keffer, and (2) in their maintenance, oversight and
7 security of their own internal databases of those internal systems to protect student
8 PII and PHI.

9 53. The University Defendants took no reasonable actions to prevent this
10 access despite their duties to students and have taken no reasonable actions to notify
11 or rectify harm to the victims of Matthew Weiss' misconduct and predation.

12 54. Thousands of students still remain at risk because the University
13 Defendants and Keffer have failed to undertake any reasonable review of how Jane
14 Doe 1's private and personal information is stored, maintained, and who can access
15 such information, and from where.

16 55. To this day, the University Defendants have not formally informed Class
17 Members impacted by Weiss' cyber sexual assault and misconduct.

18 ***University Defendants Were Negligent in Hiring/Contracting with Defendant***
19 ***Keffer and in Entrusting Students PII and PHI to Keffer***

20 56. University Defendants provided its student athletes with medical
21 treatment, including from athletic trainer employees of the University.

22 57. To facilitate that treatment, the University Defendants contracted with
23 Keffer to use its Athletic Training System application, which required that student
24 athletes provide the University Defendants and Keffer with sensitive PII and PHI.

25 58. When collecting that information, the University, like Keffer, accepted
26 an obligation to protect that information under contract and statutory principles,
27 including as a "business associate" under HIPAA.
28

1 59. Jane Doe 1 and others similar to her entrusted that the University
2 Defendants and Keffer would safeguard her private information and ensure the
3 security and confidentiality of her data.

4 60. The University Defendants and Keffer had, and continue to have, a duty
5 to protect Jane Doe 1 and to take appropriate security measures to protect private,
6 personal, medical, and intimate information, communications, and images.

7 61. The University Defendants knowingly and deliberately permitted access
8 to and the divulging of Plaintiff's stored communications through Keffer and failed
9 to take reasonable action to ensure that Keffer protected the privacy of the sensitive
10 information of Jane Doe 1 and others like her.

11 62. Upon information and belief, the University Defendants failed to properly
12 investigate Keffer, Keffer's protocols, and failed to adequately monitor or establish
13 safeguards for Keffer's work with the students and their private information to ensure
14 they carried out their duties to safeguard and protect the private information of their
15 students entrusted to them.

16 63. The University Defendants were negligent and/or reckless in failing to
17 ensure that media and other private, personal, and sensitive information, including
18 but not limited to those of Jane Doe 1, were securely protected, as the University
19 Defendants were entrusted to do.

20 64. The University Defendants failed to implement the security measures
21 necessary to protect their students PII and PHI, including failing to train staff and
22 employees on securing credentials, requiring multi-or-two-factor authentication to
23 use Keffer's Athletic Trainer System, overseeing third-party vendors like Keffer, in
24 which the University Defendants entrusted students' sensitive PII and PHI and
25 monitoring and auditing access to students' files and private information.

26 65. In other words, the University Defendants not only failed to ensure they
27 had implemented sufficient security protocols and procedures across their own
28 systems and staff, but also the University Defendants failed to ensure Keffer had

adequate security measures in place to protect its students' PII and PHI from theft and misuse.

66. Indeed, the University Defendants lacked adequate training programs to detect and stop breaches like those caused by Defendant Weiss.

67. The University Defendants and Keffer failed to implement reasonable protective measures to detect Weiss' irregular activity and trespassing, including but not limited to, appropriate authentication tools, behavioral analytics, anomaly detection, machine learning, and real-time monitoring of user activity, looking for deviations from established patterns and suspicious actions like unusual login attempts or access to sensitive data, any of which would have prevented Weiss' improper access to private student information.

68. Because Keffer and the University Defendants failed to implement basic, industry standard security measures, together these Defendants allowed an alleged sexual predator, ex-football coach Matthew Weiss, to access students', and in particular female student athletes', most sensitive information for nearly a decade.

69. All Defendants disregarded the rights of Jane Doe 1 and Class Members. The University Defendants and Keffer knowingly, intentionally, willfully, recklessly, and/or negligently provided access to and/or divulged Plaintiff's private communications stored in their facilities; failed to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failed to disclose that they did not have adequately robust computer systems and security practices to safeguard private information; failed to take standard and reasonably available steps to prevent the data breach and cyber assault; failed to properly train their staff and employees on proper security measures; failed to provide Jane Doe 1 and the Class Members prompt notice of the data breach and cyber assault.

70. Defendants University's and Keffer's conduct amounts to a violation of the duties they owed to Jane Doe 1 under common law tort claims and state and federal statutory law, rendering them liable to Jane Doe 1 and the Class Members for

1 the harms caused by this egregious and preventable cyber sexual assault and invasion
2 of privacy. Defendant Weiss is equally liable for the harms inflicted on Jane Doe 1
3 and the Class Members by his intentional hacking and exfiltration of their private
4 information under tort and statutory law.

5 71. Jane Doe 1 and the punitive Class Members are current and former
6 students at the University and other affected institutions in the United States that were
7 specifically targeted by Weiss and harmed by the violation of their privacy.

8 72. Jane Doe 1 and the punitive Class Members suffered injury as a result of
9 Defendants' conduct. These injuries included: invasion and loss of privacy, loss of
10 dignity, humiliation, embarrassment, and severe emotional distress.

11 73. Jane Doe 1 seeks to remedy these harms on behalf of herself and all
12 similarly situated individuals whose private information was accessed by Weiss.

13 74. Jane Doe 1 seeks remedies including, but not limited to, compensatory
14 damages, nominal damages, punitive damages, and reimbursement of out-of-pocket
15 costs. Jane Doe 1 also seeks injunctive and equitable relief to prevent future injury on
16 behalf of herself and the putative Class Members.

17 ***Jane Doe 1's Allegations***

18 75. Plaintiff Jane Doe 1 is a former __ student at California State University-
19 San Bernardino.

20 76. While in school at the University, Jane Doe 1 participated in the
21 Volleyball program while Defendant Weiss' data breach and cyber sexual assault was
22 ongoing.

23 77. As a student athlete, Jane Doe 1 received treatment from the University's
24 athletic trainer staff, requiring her to disclose information about her treatment,
25 including height, weight, injuries, medications, treatment plans, and analysis on
26 performance and recovery. To receive treatment, Jane Doe 1 was required to use the
27 Keffer database, and the PII and PHI Jane Doe 1 disclosed was saved on the Keffer
28 system.

1 78. As a student, Jane Doe 1 was required to disclose personal information to
2 the University and was issued a University email where sensitive, personal
3 information was stored.

4 79. Because Keffer and the University Defendants never implemented the
5 security safeguards needed to protect Jane Doe 1's PII and PHI, Defendant Weiss
6 compromised the PII and PHI belonging to every student whose information was
7 saved by the University Defendants and/or Keffer's Athletic Trainer System database,
8 including, on information and belief, Jane Doe 1's private and personal information.

9 80. Defendant Weiss compromised all information that was saved in the
10 University Defendants and/or Athletic Trainer System databases, including Plaintiff's
11 treatment information, injury information, height, weight, and other highly sensitive
12 information.

13 81. On March 26, 2025, Jane Doe 1 received notice from the U.S. Department
14 of Justice Victim Notification System that she was identified as a potential victim in
15 the federal action against Defendant Weiss.

16 82. After receiving notice from the federal government that read: "If you are
17 receiving this notification, it means that information of yours was found in possession
18 of the defendant,"¹² Jane Doe 1 felt violated, deeply disturbed, humiliated,
19 embarrassed, and extremely emotionally distressed; and is experiencing physical
20 manifestations of the stress and anxiety caused by this egregious violation of her
21 privacy – symptoms that are further exacerbated by the fact that Jane Doe 1 still does
22 not have a full and complete understanding of the data breach and cyber sexual assault
23 enabled by the University Defendants and perpetrated by Defendant Weiss.

24 83. This cyber sexual assault invaded Plaintiff's privacy and has devastated
25 her personally and emotionally, as her highly sensitive private information was stolen
26 by an alleged predator under circumstances that were preventable by University
27 Defendants and Defendant Keffer.

28 ¹² *Id.*

84. Upon information and belief, the United States Department of Justice is in the process of notifying thousands of potential victims that their privacy was breached.

85. As a direct result of the negligence, recklessness, and misconduct of the Defendants, Jane Doe 1 and those similarly situated have incurred substantial monetary and emotional harm exceeding \$5,000,000, exclusive of costs, interest, and fees.

Defendants Keffer and University Defendants Failed to Properly Protect Plaintiff's and Class Members' PII And PHI

86. Defendants Keffer and University Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted PII and PHI it was maintaining for Plaintiff and Class Members, causing the exposure of PII and PHI for 150,000 students and former students, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for approximately 3,330 students and former students.

87. The FTC promulgated numerous guides which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

88. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.¹³

¹³ *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed April 22, 2025).

1 The guidelines also recommend that businesses use an intrusion detection system to
2 expose a breach as soon as it occurs; monitor all incoming traffic for activity
3 indicating someone is attempting to hack the system; watch for large amounts of data
4 being transmitted from the system; and have a response plan ready in the event of a
5 breach.¹⁴

6 89. The FTC further recommends that companies not maintain PII and PHI
7 longer than is needed for authorization of a transaction; limit access to sensitive data;
8 require complex passwords to be used on networks; use industry-tested methods for
9 security; monitor for suspicious activity on the network; and verify that third-party
10 service providers have implemented reasonable security measures.

11 90. Defendants Keffer and the University Defendants failed to properly
12 implement the basic data security practices explained and set forth by the FTC.

13 91. Defendants Keffer's and University's failure to employ reasonable and
14 appropriate measures to protect against unauthorized access PII and PHI constitutes
15 an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

16 92. A systematic, years-long breach such as the ones Defendants Keffer and
17 the University Defendants experienced, is also considered a breach under the HIPAA
18 Rules because there is unauthorized access to PHI that is not permitted under HIPAA.

19 93. A breach under the HIPAA Rules is defined as, "the acquisition, access,
20 use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule]
21 which compromises the security or privacy of the PHI." 45 C.F.R. 164.40.

22 94. Data breaches are also Security Incidents under HIPAA because they
23 impair both the integrity (data is not interpretable) and availability (data is not
24 accessible) of patient health information:

25 ///

26 ///

27 _____
28 ¹⁴ *Id.*

The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. 45 C.F.R.164.308(a)(6).¹⁵

95. Defendants Keffer's and University's data breach was the foreseeable consequence of a combination of insufficiencies that demonstrate that Defendants Keffer and the University Defendants failed to comply with safeguards mandated by HIPAA.

University Defendants and Keffer Failed to Comply with Industry Standards

96. Defendants Keffer and the University Defendants did not utilize industry standards appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of PII and PHI for approximately 150,000 students and former students, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for 3,330 students and former students.

97. As explained by the FBI, "[p]revention is the most effective defense against cyberattacks] and it is critical to take precautions for protection."¹⁶

98. To prevent and detect cyberattacks, including the cyberattack that resulted in this prolific data breach and cyber sexual assault, Defendants could and

¹⁵ *FACT SHEET: Ransomware and HIPAA*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES (July 11, 2016), <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf> (last accessed April 22, 2025).

¹⁶ *See Ransomware Prevention and Response for CISOs*, FBI, <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last accessed April 22, 2025).

1 should have implemented, as recommended by the United States Government, the
2 following measures:

- 3 • Implement an awareness and training program. Because end users are
4 targets, employees and individuals should be aware of the threat of
5 cyberattacks and how it is delivered.
- 6 • Enable strong spam filters to prevent phishing emails from reaching the
7 end users and authenticate inbound email using technologies like Sender
8 Policy Framework (“SPF”), Domain Message Authentication Reporting
9 and Conformance (“DMARC”), and DomainKeys Identified Mail
10 (“DKIM”) to prevent email spoofing.
- 11 • Scan all incoming and outgoing emails to detect threats and filter
12 executable files from reaching end users.
- 13 • Configure firewalls to block access to known malicious IP addresses.
- 14 • Patch operating systems, software, and firmware on devices. Consider
15 using a centralized patch management system.
- 16 • Set anti-virus and anti-malware programs to conduct regular scans
17 automatically.
- 18 • Manage the use of privileged accounts based on the principle of least
19 privilege: no users should be assigned administrative access unless
20 absolutely needed; and those with a need for administrator accounts should
21 only use them when necessary.
- 22 • Configure access controls—including file, directory, and network share
23 permissions—with least privilege in mind. If a user only needs to read
24 specific files, the user should not have written access to those files,
25 directories, or shares.
- 26 • Disable macro scripts from office files transmitted via email. Consider
27 using Office Viewer software to open Microsoft Office files transmitted
28 via email instead of full office suite applications.

- Implement Software Restriction Policies (“SRP”) or other controls to prevent programs from executing from common cyberware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (“RDP”) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.¹⁷

99. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the data breach and cyber sexual assault, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (“Oss”) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the Internet for the sender organization’s website or the topic mentioned in

¹⁷ *Id.* at 3-4.

the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net).

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it....
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.¹⁸

100. To prevent and detect cyberattacks, including the cyberattack that resulted in the data breaches and cyber sexual assaults, Defendants Keffer and the University

¹⁸ See *Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Sep. 2, 2021), <https://www.cisa.gov/news-events/news/protecting-against-ransomware> (last accessed April 22, 2025).

Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure Internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].¹⁹

101. As described above, experts studying cyber security routinely identify medical facilities as being particularly vulnerable to cyberattacks because of the value of the private information they collect and maintain.

102. Several best practices have been identified that at a minimum should be implemented by institutions such as Defendants Keffer and University, including, but not limited to, the following: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

103. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

104. Given that Defendants Keffer and the University Defendants were storing the private information of 150,000 individuals combined, Defendants Keffer and the University Defendants could and should have implemented all of the above measures to prevent cyberattacks, along with the two-or multi-factor authentication discussed earlier in this Complaint.

105. The occurrence, scope, and duration of the breach and cyber sexual assaults indicate that Defendants Keffer and the University Defendants failed to

¹⁹ See Microsoft Threat Intelligence, *Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (March 5, 2020), <https://www.microsoft.com/en-us/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last accessed April 22, 2025).

adequately implement one or more of the above measures to prevent cyberattacks, resulting in the exposure of approximately 150,000 students' and former students' PII and PHI, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for 3,330 students and former students.

Defendants Keffer and the University Defendants Failed to Properly Protect PII and PHI

106. Defendants Keffer and the University Defendants breached their obligations to Jane Doe 1 and Class Members and were otherwise grossly negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches, cyber-attacks, hacking incidents, and ransomware attacks;
- b. Failing to adequately protect students' private information;
- c. Failing to properly monitor its own data security systems for existing or prior intrusions;
- d. Failing to test and assess the adequacy of its data security system;
- e. Failing to develop adequate training programs related to the proper handling of emails and email security practices;
- f. Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;
- g. Failing to require a data security system to ensure the confidentiality and integrity of electronic PHI its network created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- h. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information

1 to allow access to only those persons or software programs that have been
2 granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

3 i. Failing to implement policies and procedures to prevent, detect, contain,
4 and correct security violations in violation of 45 C.F.R. §
5 164.308(a)(1)(i);

6 j. Failing to implement procedures to review records of information system
7 activity regularly, such as audit logs, access reports, and security incident
8 tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

9 k. Failing to protect against reasonably anticipated threats or hazards to the
10 security or integrity of electronic PHI in violation of 45 C.F.R. §
11 164.306(a)(2);

12 l. Failing to protect against reasonably anticipated uses or disclosures of
13 electronic PHI that are not permitted under the privacy rules regarding
14 individually identifiable health information in violation of 45 C.F.R. §
15 164.306(a)(3);

16 m. Failing to ensure that it was compliant with HIPAA security standard
17 rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

18 n. Failing to train all members of its workforce effectively on the policies
19 and procedures regarding PHI as necessary and appropriate for the
20 members of its workforce to carry out their functions and to maintain
21 security of PHI, in violation of 45 C.F.R. § 164.530(b);

22 o. Failing to ensure that the electronic PHI it maintained is unusable,
23 unreadable, or indecipherable to unauthorized individuals, as Defendants
24 had not encrypted the electronic PHI as specified in the HIPAA Security
25 Rule by “the use of an algorithmic process to transform data into a form in
26 which there is a low probability of assigning meaning without use of a
27 confidential process or key” (45 C.F.R. §164.304 definition of encryption);
28

- p. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;
- q. Failing to adhere to industry standards for cybersecurity.

107. As the result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendants Keffer and the University Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' private, sensitive information.

108. The University Defendants were also grossly negligent in their failure to oversee the data security practices of third-party vendor—Keffer—in which they entrusted the sensitive private information of their students and former students.

109. Accordingly, as outlined below, Plaintiff and Class Members have already been severely harmed by this egregious violation of their privacy by Defendant Weiss.

Defendants Caused Plaintiff and the Class Members to Suffer Loss of Privacy and Dignitary Harm

110. Defendants' conduct enabled a significant violation of privacy, extending far beyond the mere loss of data. The type of information compromised ranged from personal information like names, contact information and passwords to medical and psychological information and intimate photos and communications that were never meant for public viewing or viewing by an unauthorized third party. When extremely sensitive personal information such as this is compromised, individuals face a cascade of potential harm that erodes their sense of security and control, as information that they thought would remain confidential and private has now been leaked to the outside world, and which they no longer exercise control over. This exposure can lead to a profound sense of vulnerability, as individuals grapple with the knowledge that their most personal details are now in the hands of unknown actors, free to circulate and be publicized now, or at any time in the future.

111. Information regarding an individual's health and medical choices, such as here, as well as private communications and intimate photos meant for a romantic partner are among the most sensitive information there is. An individual's right to privacy regarding their body, their medical and psychological care, their romantic interests and their sexual and intimate life are the most sacrosanct and inviolable rights an individual possesses, striking to the very core of their personhood and dignity. Harm relating to an individual's loss of privacy and dignitary harm, especially with information as sensitive as this, has also long been recognized by courts and in the common law.

112. When an individual loses this privacy and such sensitive information is viewed by a third party without their knowledge or consent, this harm cannot be undone. Weiss' unlawful and immoral violation of the personal and intimate lives of thousands of young people shocks the conscience and causes humiliation and loss of dignity that cannot be easily undone. The University Defendants and Keffer's failure to safeguard this sensitive information has stripped Plaintiff and the Class Members of this essential control, exposing them to the potential for enduring emotional distress and the profound sense of vulnerability that accompanies the exposure of deeply private matters.

113. By stripping Plaintiff and the Class Members of their right to control this sensitive information about themselves, Defendants have done immense harm to Plaintiff and the Class Members' rights to privacy as well as their personal dignity and bodily sovereignty. This permanent loss of security and fundamental right to privacy and bodily autonomy is harm that no compensation can ever fully restore.

V. TOLLING

114. Plaintiff realleges and incorporate by reference all preceding allegations as though fully set forth herein.

1 115. The statutes of limitations applicable to Plaintiff's claims were tolled by
2 Defendants' conduct and Plaintiff's and Class Members delayed discovery of their
3 claims.

4 116. As alleged above, Plaintiff did not know, and could not have known, that
5 Defendant Weiss would have surreptitiously obtained her personal photographs and
6 information without her consent.

7 117. The Defendants' alleged unlawful conduct could not have been
8 discovered until at least March 2025 when Plaintiff was notified by the Department
9 of Justice that her information was found in possession of Weiss who obtained it
10 through illegal means.

11 118. Plaintiff could not have discovered, through the exercise of reasonable
12 diligence, the full scope of Defendants' alleged unlawful conduct, as Weiss
13 surreptitiously accessed her information and the other Defendants failed to stop him
14 or otherwise make Plaintiff and the Class Members aware of this illegal activity.

15 119. All applicable statutes of limitations have been tolled by operation of the
16 delayed discovery rule. Under the circumstances, Defendants were under a duty to
17 disclose the nature and significance of the invasion of privacy but did not do so.
18 Defendants are therefore estopped from relying on any statute of limitations.

19 **VI. CLASS ALLEGATIONS**

20 120. Plaintiff files this lawsuit both individually and as representative of all
21 others similarly situated pursuant to Fed. R. Civ. P. 23 on behalf of the following
22 Class:

23 **Nationwide Class:**

24
25 All students whose personal data, images, information, social media, or videos
26 were accessed by Weiss without authorization (the "Class Members").

27 121. In addition, Plaintiff believes a subclass may be appropriate for all class
28 members who receive notice from the United States Department of Justice as to the

likely violation of their privacy and rights by Weiss. Therefore, Plaintiff pleads a subclass as follows:

California Subclass:

All students whose personal data, images, information, social media, or videos were accessed by Weiss without authorization and who received a notice letter from the United States Department of Justice as to Weiss (the “DOJ Letter Sub-Class”).

122. Excluded from the Class are: (a) Defendants and any entity or division in which Defendants have a controlling interest, and their legal representatives, officers, directors, assigns, and successors; (b) the Judge to whom this case is assigned and the Judge’s staff; and (c) the attorneys representing any parties to this Class Action.

123. Plaintiff reserves the right to modify or amend the definition of the proposed class and/or sub-classes before the Court determines whether certification is appropriate.

124. The requirements of Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3) are met in this case.

125. The Fed. R. Civ. P. 23(a) elements of Numerosity, Commonality, Typicality, and Adequacy are all satisfied.

126. **Numerosity:** Law enforcement officials have disclosed the numbers of victims is significant and exceeds one thousand, satisfying the numerosity requirement. Although the exact number of Class Members is uncertain at this time, it will certainly be ascertained through appropriate discovery and the number is great enough such that joinder is impracticable.

127. The members of the Class are so numerous and geographically disperse that individual joinder of all members is impracticable.

1 128. Similarly, Class members may be notified of the pendency of this action
2 by recognized, Court-approved notice dissemination methods, which may include
3 U.S. mail, electronic mail, internet postings, and/or published notice.

4 129. Class Members are readily identifiable from information and records in
5 the possession of the federal and state authorities, the University, and Keffer.

6 130. Electronic records maintained by the University Defendants and Keffer
7 can confirm the identification of Class Members.

8 131. **Commonality:** Defendants engaged in a common course of conduct
9 giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself
10 and the other Class Members. Similar or identical violations, practices, and injuries
11 are involved, and the burden of proof to establish violations of those rights involve
12 uniform, objective questions of fact and law, both for the prosecution and for the
13 defense.

14 132. The common questions of fact and law existing as to all Class Members
15 predominate over questions affecting only individual class members. The evidence
16 required to advance Plaintiff's and Class Members' claims are the same, common to
17 all; as is true of the evidence Defendants will likely rely upon in defense of this action.
18 Thus, the elements of commonality and predominance are both met.

19 133. For example, establishing the facts of how, where, who, when, and
20 through what means the invasions of Plaintiff's and other Class Members occurred
21 are identical.

22 134. Defendants' actions, inactions, negligence, and recklessness apply
23 commonly to Plaintiff and Class Members.

24 135. The downloads and invasions by Weiss and the improper conduct
25 accessing private information through unsecure facilities without permission is
26 common to all Class Members and has caused injury to the Plaintiff and Class
27 Members in common manners.
28

1 136. The majority of legal and factual issues of the Plaintiff and the Class
2 Members predominate over any individual questions, including:

- 3 (a) Whether Defendants unlawfully used, maintained, lost, or
4 disclosed Plaintiff's and Class Members private information;
- 5 (b) Whether Defendants Keefer and the University Defendants failed
6 to implement and maintain reasonable security procedures and
7 practices appropriate to the nature and scope of the information
8 compromised in the hacking incident and cyber sexual assault;
- 9 (c) Whether Defendants Keefer and the University's data security
10 systems prior to and during the data breach and cyber sexual assault
11 complied with applicable data security laws and regulations;
- 12 (d) Whether Defendants Keefer's and the University's data security
13 systems prior to and during the data breach and cyber sexual assault
14 were consistent with industry standards;
- 15 (e) Whether Defendants Keefer and the University Defendants owed a
16 duty to Plaintiff and Class Members to safeguard their private
17 information;
- 18 (f) Whether Defendants Keefer and the University Defendants
19 breached their duty to Plaintiff and Class Members to safeguard
20 their private information;
- 21 (g) Whether the University Defendants were grossly negligent and/or
22 negligent in their oversight of Defendant Keffer;
- 23 (h) Whether the University Defendants or Keffer knew or should have
24 known that their data security systems and monitoring processes
25 were deficient;
- 26 (i) Whether Defendants Keefer and the University Defendants owed a
27 duty to provide Plaintiff and Class Members timely notice of the
28 data breach and cyber sexual assaults, and whether Defendants

Keefer and the University Defendants breached that duty to provide timely notice;

(j) Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

(k) Whether Defendants' conduct was negligent or grossly negligent;

(l) Whether Defendants' conduct was per se negligent;

(m) Whether Defendants' conduct violated federal laws;

(n) Whether Defendants' conduct violated state laws;

(o) Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or punitive damages; and

(p) Other common questions of fact and law relative to this case that remain to be discovered.

137. Resolving the claims of these Class Members in a single action will provide benefit to all parties and the Court by preserving resources, avoiding potentially inconsistent results, and providing a fair and efficient manner to adjudicate the claims.

138. Predominance does not require Plaintiff to prove an absence of individualized damage questions, or even proof of class wide damage in the aggregate. *Kuchar v. Saber Healthcare Holdings LLC*, 340 F.R.D. 115, 123 (N.D. Ohio 2021) (finding individualized damages questions also do not defeat a predominance finding and noting "when adjudication of questions of liability common to the class will achieve economies of time and expense, the predominance standard is generally satisfied even if damages are not provable in the aggregate.") (citing *Hicks v. State Farm Fire & Cas. Co.*, 965 F.3d 460 (6th Cir. 2020).)

139. **Typicality:** Plaintiff's claims are typical of those of other Class Members because all had their private information compromised as a result of the breach and cyber assault and Defendants' malfeasance.

1 140. Plaintiff's claims are typical of the Class Members because they are
2 highly similar and the same and related in timing, circumstance, and harm suffered.
3 To be sure, there are no defenses available to Defendants that are unique to individual
4 Plaintiff. The injury and causes of actions are common to the Class as all arising from
5 the same statutory and privacy interests.

6 141. In *Halliburton Co. v. Erica P. John Fund, Inc.*, 573 U.S. 258, 276 (2014)
7 the Supreme Court concluded that so long as Plaintiff could show that their evidence
8 is capable of proving the key elements to Plaintiff's claim on a class-wide basis, the
9 fact that the defendants would have the opportunity at trial to rebut that presumption
10 as to some of the Plaintiff did not raise individualized questions sufficient to defeat
11 predominance. "That the defendant might attempt to pick off the occasional class
12 member here or there through individualized rebuttal does not cause individual
13 questions to predominate." *Id.*

14 142. Certification of Plaintiff's claims for class-wide treatment is appropriate
15 because Plaintiff can prove the elements of her claims on a class-wide basis using the
16 same evidence as would be used to prove those elements in individual actions alleging
17 the same claims.

18 143. The need to conduct additional post certification stage discovery, such as
19 further file review or class member surveys, to eliminate uninjured persons after trial,
20 does not act as a *de facto* bar to certification. *Nixon*, 2021 WL 4037824, at *8 (citing
21 *Young*, 693 F.3d at 540); *In re Visa Check/MasterMoney Antitrust Litig.*, 280 F.3d
22 124, 145 (2d Cir. 2001); *Perez v. First Am. Title Ins. Co.*, 2009 WL 2486003, at *7
23 (D. Ariz. Aug. 12, 2009) ("Even if it takes a substantial amount of time to review files
24 and determine who is eligible for the [denied] discount, that work can be done through
25 discovery."); *Slapikas v. First Am. Title Ins. Co.*, 250 F.R.D. 232, 250 (W.D. Pa.
26 2008) (finding class action manageable despite First American's assertion that "no
27 database exists easily and efficiently to make the determination that would be required
28 for each file").

1 144. Any remaining disputes on membership or class members damages can
2 be left to a special master's decision. *Whitlock v. FSL Mgmt., LLC*, 2012 WL
3 3274973, at *12 (W.D. Ky., 2012), *aff'd*, 843 F.3d 1084 (6th Cir. 2016). By placing
4 the validation of injury step at the end of the class trial process, no injured class
5 members are left out, and at the same time, Defendants are not at risk for paying any
6 uninjured class members.

7 145. **Adequacy:** Plaintiff will fairly and adequately represent and protect the
8 interests of the Class Members in that she has no interests that are in conflict with
9 those of the Class Members. In addition, she has retained counsel competent and
10 experienced in complex class action litigation, and she will prosecute this action
11 vigorously. The Class's interests will be fairly and adequately protected by Plaintiff
12 and her counsel.

13 146. **Superiority:** The class action is superior to any other available
14 procedures for the fair and efficient adjudication of these claims, and no unusual
15 difficulties are likely to be encountered in the management of this class action.

16 147. The superiority analysis required to certify a class is designed to achieve
17 economies of time, effort and expense, and to promote uniformity of decisions as to
18 persons similarly placed, without sacrificing procedural fairness or bringing about
19 other undesirable results.

20 148. A class action is superior to all other available methods for the fair and
21 efficient adjudication of this controversy since joinder of all members is
22 impracticable.

23 149. It would be an unnecessary burden upon the court system to require these
24 individual Class Members to institute separate actions. Individualized litigation
25 creates a potential for inconsistent or contradictory judgments and increases the delay
26 and expense to all parties and the court. By contrast, the class action device presents
27 far fewer management difficulties and provides the benefits of a single adjudication,
28 economy of scale, and comprehensive supervision by a single court.

1 150. Pursuing this matter as a class action is superior to individual actions
2 because:

- 3 (a) Separate actions by Class Members could lead to inconsistent or
4 varying adjudications that would confront Defendants with
5 potentially incompatible standards of conduct;
6 (b) Many victims will not come forward without a certified class;
7 (c) Final equitable relief will be appropriate with respect to the entire
8 Class as a whole for monitoring, protection, therapy and other
9 equitable forms of relief that may be provided;
10 (d) This action is manageable as a class action and would be
11 impractical to adjudicate any other way;
12 (e) Absent the class action, individual Class Members may not know
13 if their privacy was invaded; where such images are currently being
14 stored, or are accessible by others; and their injuries are likely to
15 go unaddressed and unremedied; and,
16 (f) Individual Class members may not have the ability or incentive to
17 pursue individual legal action on their own.

18 151. **Particular Issues:** In the event unforeseen issues preclude class
19 certification under Fed.R.Civ.P. 23(b)(3), the case is still appropriate for class
20 certification under Fed.R.Civ.P. 23(c)(4), as to the particular issues of liability.

21 152. Defendants have acted or refused to act on grounds generally applicable
22 to Plaintiff and the other members of the Class, thereby making declaratory relief, as
23 described below, with respect to the Class as a whole.

24 ///

25 ///

26 ///

27 ///

28 ///

COUNT ONE

VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT – 18 U.S.C. §

1030

(Against Defendant Weiss)

153. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

154. Plaintiff alleges that Defendant Weiss violated the Computer Fraud and Abuse Act.

155. Weiss violated the Computer Fraud and Abuse Act by unlawfully accessing Plaintiff's private information without authorization.

156. Weiss' actions constituted a violation of the Act because by entering the digital network and extracting sensitive private information of students, he "intentionally accesse[d] a computer without authorization" 18 U.S.C. § 1030(a)(2)(C).

157. Weiss' actions were deliberate because he knew he was unauthorized and proceeded, nevertheless.

158. Under 18 U.S.C. § 1030(g), Plaintiff may recover damages in this civil action from Weiss along with injunctive relief or other equitable relief.

159. Given the willful violations committed by Weiss, resulting in significant damage, harm, humiliation, and distress to Plaintiff and other Class Members, Plaintiff should be awarded all appropriate damages in this matter.

COUNT TWO

VIOLATIONS OF THE STORED COMMUNICATIONS ACT

U.S.C. § 2701 et seq.

(Against Defendants Weiss, Keffer and the University Defendants)

160. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

1 161. Plaintiff alleges that Defendants Weiss, Keffer and the University
2 Defendants violated the Stored Communications Act.

3 162. The Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, prohibits the
4 unauthorized access of web-based cloud storage and media accounts such as those at
5 issue and other accounts hosted by the University Defendants and Keffer that contain
6 personal, private, and intimate information and communications about and relating to
7 Plaintiff and others situated similarly to Plaintiff.

8 163. Specifically, under 18 U.S.C. § 2701(a), it is unlawful for any person to:
9 (1) intentionally access without authorization a facility through which an electronic
10 communication service is provided; or (2) intentionally exceed an authorization to
11 access that facility; and thereby obtain, alter, or prevent authorized access to a wire
12 or electronic communication while it is in electronic storage in such system.

13 164. Under 18 U.S.C. § 2702, it is unlawful for a person or entity providing an
14 electronic communication service to the public to knowingly divulge to any person
15 or entity the contents of a communication while in electronic storage by that service
16 or to divulge to any person or entity the contents of any communication which is
17 carried or maintained on that service on behalf of a subscriber or customer of such
18 service, solely for the purpose of providing storage or computer processing services
19 to such subscriber or customer, if the provider is not authorized to access the contents
20 of any such communications for purposes of providing any services other than storage
21 or computer processing.

22 165. Plaintiff's electronic information and communications were in electronic
23 storage and clearly fall within the scope of the statute.

24 166. Defendant Weiss was not authorized to access or divulge the content of
25 Plaintiff's private communications for any purpose; and yet, the University
26 Defendants and Keffer enabled Weiss to access Plaintiff's electronic information and
27 communications.
28

1 167. The information, messages, files, and media were accessed by Weiss
2 without authorization.

3 168. Weiss' access without authorization was deliberate.

4 169. There is no manner in which Plaintiff's private information, messages,
5 files, and media could have been obtained without unauthorized access and would not
6 have been obtained without unauthorized access had the University Defendants and
7 Keffer not knowingly divulged or permitted access to such information, through
8 Keffer Development other channels, despite knowing that the information would not
9 be protected.

10 170. Under Section 2707 of the Stored Communications Act, individuals may
11 bring a civil action for the violation of this statute.

12 171. This law imposes strict liability on violators.

13 172. The statute provides that a person aggrieved by a violation of the act may
14 seek appropriate relief including equitable and declaratory relief, actual damages or
15 damages no less than \$1,000 punitive damages, and reasonable attorney's fee[s] and
16 other litigation costs reasonably incurred according to 18 U.S.C. § 2707(b)-(c).

17 173. Defendants' access to and divulging of Plaintiff's private, personal, and
18 intimate information, messages, files, and media constituted a violation of 18 U.S.C.
19 §§ 2701 and 2702.

20 174. The University Defendants, Keffer and Weiss knew they did not have
21 authority to access and divulge Plaintiff's private, personal, and intimate information,
22 messages, files, and media but did so anyway.

23 175. Defendants' knowing or intentional conduct led to multiple violations of
24 the Stored Communications Act.

25 176. As a result of these violations, Plaintiff has incurred significant monetary
26 and nonmonetary damages as a result of these violations of the Stored
27 Communications Act, and Plaintiff seeks appropriate compensation for her damages.
28

1 177. Under the statute, Plaintiff should be granted the greater of (1) the sum of
2 her actual damages suffered and any profits made by the University Defendants,
3 Keffer and Weiss as a result of the violations or (2) \$1,000 per violation of the Stored
4 Communications Act.

5 178. Given these violations were deliberate, the Court should assess punitive
6 damages against Defendants as well.

7 179. Plaintiff should also be granted reasonable attorney fees and costs.

8 **COUNT THREE**

9 **VIOLATION OF TITLE IX, 20 U.S.C. § 1681(A) *et seq.***

10 ***(Against Defendants Trustees and the University)***

11 180. Plaintiff restates and incorporates the allegations set forth above as if fully
12 set forth herein.

13 181. Plaintiff alleges that the University Defendants violated Title IX, 20
14 U.S.C. § 1681(A) *et seq.*

15 182. These Defendants receive federal financial support for their educational
16 programs and are therefore subject to the provisions of Title IX of the Education Act
17 of 1972, 20 U.S.C. § 1681(a), *et seq.*

18 183. Title IX mandates that “No person in the United States shall on the basis
19 of sex, be ... subject to discrimination under any education program or activity
20 receiving Federal financial assistance ...”

21 184. Each Plaintiff and Class Member is a “person” under the Title IX
22 statutory language.

23 185. Weiss specifically targeted women in his unwanted invasions of privacy
24 and his misconduct is discrimination on the basis of sex.

25 186. The University Defendants, under Title IX, are obligated to investigate
26 allegations of sexual harassment.

27 187. The University Defendants were aware of the sensitive nature of the
28 private and personal information of Plaintiff to which Weiss was able to access.

1 188. The University Defendants acted with deliberate indifference to sexual
2 harassment by:

- 3 a. Failing to protect Plaintiff and others as required by Title IX;
4 b. Neglecting to adequately investigate and address the complaints
5 regarding the deeply sensitive information Plaintiff provided;
6 c. Failing to institute corrective measures to prevent Weiss from sexually
7 harassing students; and
8 d. Failing to adequately investigate the other multiple acts of deliberate
9 indifference.

10 189. The University Defendants acted with deliberate indifference as their lack
11 of response to the sexual harassment was clearly unreasonable in light of the known
12 circumstances.

13 190. The University Defendants' failure to promptly and appropriately protect,
14 investigate, and remedy and respond to the sexual harassment of women has
15 effectively denied them equal educational opportunities at the University, including
16 access to medical care and sports training.

17 191. At the time the Plaintiff received some medical and/or athletic training
18 services from the University, she did not know the Defendants failed to adequately
19 consider her safety.

20 192. As a result of the University Defendants' deliberate indifference, Plaintiff
21 have suffered loss of educational opportunities and/or benefits.

22 193. Plaintiff has incurred, and will continue to incur, attorney's fees and costs
23 of litigation.

24 194. At the time of the University Defendants' misconduct and wrongful
25 actions and inactions, Plaintiff was unaware, and or with reasonable diligence could
26 not have been aware, of Defendants' institutional failings with respect to their
27 responsibilities under Title IX.
28

203. At the time of his actions giving rise to this count, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally searched and seized Plaintiff's private information without her consent, without a warrant, without probable cause or reasonable suspicion, and without any lawful basis or justification, in violation of Plaintiff's clearly established rights under the Fourth Amendment.

204. The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."

205. It is well settled that the Fourth Amendment's protection extends beyond the sphere of criminal investigations. *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 755 (2010) (citing *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 530 (1967)).

206. "The [Fourth] Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government, without regard to whether the government actor is investigating crime or performing another function." *Id.* (quoting *Skinner v. Railway Labor Executives' Assn.*, 489 U.S. 602, 613-614 (1989)).

207. Plaintiff had a reasonable and legitimate expectation of privacy in her private, personal, and intimate information and images.

208. Acting under color of law, Defendant Weiss violated Plaintiff's clearly established right not to have her private, personal, and intimate information and images accessed, searched, viewed, and seized when he searched and seized Plaintiff's private, personal, and intimate information and images without a warrant, without reasonable suspicion, without probable cause, and without any lawful basis, justification or need to support such an intrusion on Plaintiff's reasonable and legitimate expectation of privacy in that information.

209. Defendant Weiss’ search and seizure of Plaintiff’s personal information was per se unreasonable under the Fourth Amendment.

210. Defendant Weiss’ search and seizure of Plaintiff’s private, personal, and intimate information and images was unjustified at its inception and was not related in scope to any circumstances that would justify the search and seizure in the first place.

211. Defendant Weiss is not entitled to qualified immunity because Plaintiff’s rights under the Fourth Amendment not to have her personal information searched and seized by him without a warrant, without permission, and without any lawful basis or justification, was obvious and clearly established when Weiss accessed Plaintiff’s private information, such that no reasonable person in Weiss’ position would believe that the act of searching and seizing Plaintiff’s private information was lawful under the specific circumstances presented, and Weiss had fair warning under the law as it existed at the time of his actions that those actions obviously violated Plaintiff’s rights under the Fourth Amendment. See, e.g., *G.C. v. Owensboro Public Schools*, 711 F.3d 623 (6th Cir. 2013) (Holding that high school officials violated the Fourth Amendment by searching a student’s cell phone and reading his text messages); see also *Brannum v. Overton County School Bd.*, 516 F.3d 489, 499 (Stating that “Some personal liberties are so fundamental to human dignity as to need no specific explication in our Constitution in order to ensure their protection against government invasion[,]” and holding that school officials violated Fourth Amendment by installing cameras to surreptitiously record students in locker rooms.)

212. As a direct and proximate result of Weiss’ violation of Plaintiff’s Fourth Amendment rights, Plaintiff has suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

213. Plaintiff should be awarded all such forms of damages in this case for Weiss’ conduct that caused great damage, humiliation, and embarrassment to Plaintiff and the Class.

COUNT FIVE

VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.

§ 1983 - DUE PROCESS/BODILY INTEGRITY

(Against Defendant Weiss)

214. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

215. Plaintiff is alleging Defendant Weiss violated her civil rights under 42 U.S.C. § 1983 and the Fourteenth Amendment of the U.S. Constitution.

216. On information and belief, Defendant Weiss, sued in his individual capacity, was a state employee at all times relevant to this Count, and acted under color of state law to deprive Plaintiff of her “rights, privileges or immunities secured by the Constitution and laws” of the United States, 42 U.S.C. § 1983, specifically her Fourteenth Amendment equal protection right to be free from sexual harassment in an educational setting, and her Fourteenth Amendment due process right to be free from violation of bodily integrity. *West v. Atkins*, 487 U.S. 42, 49-50 (1988) (quoting *Lugar v. Edmondson Oil Co.*, 457 U.S. 922, 936 n. 18 (1982)).

217. At the time of the actions giving rise to this Count, it was obvious, clearly established, and known to Weiss that the right to be free from sexual abuse at the hands of a state employee was protected by the Due Process Clause of the Fourteenth Amendment, such that he knew his actions in accessing Plaintiff’s private, personal, and intimate information and images violated Plaintiff’s fundamental right of due process. *Doe v. Claiborne Cnty., Tenn. By & Through Claiborne Cnty. Bd. of Educ.*, 103 F.3d 495, 506-07 (6th Cir. 1996) (Stating that “the Due Process Clause protects students against abusive governmental power as exercised by a school. To be sure, the magnitude of the liberty deprivation that sexual abuse inflicts upon the victim is an abuse of governmental power of the most fundamental sort; it is an unjustified intrusion that strips the very essence of personhood. If the “right to bodily integrity” means anything, it certainly encompasses the right not to be sexually assaulted under

1 color of law. This conduct is so contrary to fundamental notions of liberty and so
2 lacking of any redeeming social value, that no rational individual could believe that
3 sexual abuse by a state actor is constitutionally permissible under the Due Process
4 Clause.”).

5 218. On information and belief, at the time of his actions giving rise to this
6 Count, Weiss was a state actor, functioning in his capacity as a coach and employee
7 of the University of Michigan, when he intentionally engaged in actions which
8 violated Plaintiff’s right of bodily integrity, in violation of the Due Process Clause.

9 219. Weiss’ actions were malicious, intentionally harmful, and were taken
10 with deliberate indifference, and were so outrageous as to shock the contemporary
11 conscience.

12 220. As a direct and proximate result of Weiss’ violation of Plaintiff’s
13 Fourteenth Amendment rights, Plaintiff has suffered, and will continue to suffer into
14 the future, damage, humiliation, and embarrassment.

15 221. Plaintiff should be awarded all such forms of damages in this case for
16 Weiss’ conduct that caused great damage, humiliation, and embarrassment to Plaintiff
17 and the Class.

18 **COUNT SIX**

19 **VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.**

20 **§ 1983 - EQUAL PROTECTION**

21 ***(Against Defendant Weiss)***

22 222. Plaintiff restates and incorporates the allegations set forth above as if fully
23 set forth herein.

24 223. Plaintiff is alleging Defendant Weiss violated her civil rights under 42
25 U.S.C. § 1983 and the Fourteenth Amendment of the U.S. Constitution.

26 224. Weiss’ deliberate and intentional actions in accessing Plaintiff’s personal,
27 private, and intimate images and information constituted sexual harassment and abuse
28

1 because Weiss accessed Plaintiff's highly sensitive, private, and personal
2 information, data, and media for his own personal and sexual purposes.

3 225. At the time of the actions giving rise to this case, it was obvious, clearly
4 established, and known to Weiss that the right to be free from gender discrimination,
5 including sexual harassment and abuse at the hands of a state employee, was protected
6 by the Equal Protection Clause of the Fourteenth Amendment, such that Weiss knew
7 his actions in accessing Plaintiff's personal, private, and intimate images and
8 information violated Plaintiff's rights under the Fourteenth Amendment. *Fitzgerald*
9 *v. Barnstable Sch. Comm.*, 555 U.S. 246, 257-258 (2009); see also *Daniels v. Board*
10 *of Education*, 805 F.2d 203, 206-07 (6th Cir.1986); *Gutzwiller v. Fenik*, 860 F.2d
11 1317, 1325 (6th Cir. 1988); *Kitchen v. Chippewa Valley Sch.*, 825 F.2d 1004, 1012
12 (6th Cir. 1987).

13 226. On information and belief, at the time of his actions giving rise to this
14 Count, Weiss was a state actor, functioning in his capacity as a coach and employee
15 of the University of Michigan, when he intentionally engaged in sexual harassment
16 and sexual abuse, in violation of the Equal Protection Clause.

17 227. As a direct and proximate result of Weiss' violation of Plaintiff's
18 Fourteenth Amendment rights, Plaintiff has suffered, and will continue to suffer into
19 the future, damage, humiliation, and embarrassment.

20 228. Plaintiff should be awarded all such forms of damages in this case for
21 Weiss' conduct that caused great damage, humiliation, and embarrassment to Plaintiff
22 and the Class.

23 **COUNT SEVEN**

24 **VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.**

25 **§ 1983 - DUE PROCESS/DEPRIVATION OF PROPERTY**

26 ***(Against Defendant Weiss)***

27 229. Plaintiff restates and incorporates the allegations set forth above as if fully
28 set forth herein.

230. Plaintiff alleges that Defendant Weiss violated her civil rights under 42 U.S.C. § 1983 and the Fourteenth Amendment of the U.S. Constitution.

231. On information and belief, Defendant Weiss, sued in his individual capacity, was a state employee at all times relevant to this Count, and acted under color of state law to deprive Plaintiff of her “rights, privileges or immunities secured by the Constitution and laws” of the United States, 42 U.S.C. § 1983, specifically her Fourteenth Amendment due process right to be free of deprivations of property without due process

232. At the time of the actions giving rise to this case, it was obvious, clearly established, and known to Weiss that the right not to be deprived of one’s property without due process was protected by the Due Process Clause of the Fourteenth Amendment, such that he knew his actions in accessing and misappropriating Plaintiff’s private, personal, and intimate information and images violated Plaintiff’s fundamental right of due process.

233. Plaintiff and others similarly situated had a protected property interest in their personal, private, intimate, and confidential information.

234. At the time of his actions giving rise to this case, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally engaged in actions which violated Plaintiff’s right not to be deprived of her personal property, in violation of the Due Process Clause.

235. Weiss’ actions were malicious, intentionally harmful, and were taken with deliberate indifference, and were so outrageous as to shock the contemporary conscience.

236. As a direct and proximate result of Weiss’ violation of Plaintiff’s Fourteenth Amendment rights, Plaintiff has suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

237. Plaintiff should be awarded all such forms of damages in this case for Weiss' conduct that caused great damage, humiliation, and embarrassment to Plaintiff and the Class.

COUNT EIGHT
INVASION OF PRIVACY
(Against all Defendants)

238. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

239. Plaintiff and the Class Members had a reasonable and legitimate expectation of privacy in their Private Information that the Defendants failed to adequately protect against compromise from unauthorized third parties.

240. The Defendants owed a duty to Plaintiff and Class Members to keep their Private Information confidential.

241. Defendant Keffer and the University Defendants failed to protect and allowed the Private Information of Plaintiff and Class Members to be exfiltrated and stolen by Defendant Weiss.

242. Defendant Weiss additionally invaded the Privacy of Plaintiff and the Class Members by secretly obtaining their Private Information as well as photos, communications, and other information for his own personal and illicit use without the knowledge or consent of Plaintiff or the Class Members.

243. By failing to keep Plaintiff's and Class Members' Private Information safe, knowingly utilizing unsecure systems and practices, Defendants unlawfully invaded Plaintiff's and Class Members' privacy by, among others, (i) intruding into Plaintiff's and Class Members' private affairs in a manner that would be highly offensive to a reasonable person; (ii) failing to adequately secure their Private Information from disclosure to unauthorized persons and/or third parties; and (iii) enabling the disclosure of Plaintiff's and Class Members' Private Information without consent.

244. Defendants knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's and Class Members' position would consider their actions highly offensive.

245. The University Defendants and Keffer knew, or acted with reckless disregard of the fact that, organizations handling PII or PHI are highly vulnerable to cyberattacks and that employing inadequate security and training practices would render them especially vulnerable to data breaches.

246. As a proximate result of such unauthorized disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted, thereby causing Plaintiff and the Class Members undue harm.

247. Plaintiff seeks injunctive relief on behalf of the Class, restitution, as well as any and all other relief that may be available at law or equity. Unless and until enjoined, and restrained by order of this Court, the Defendants' wrongful conduct will continue to cause irreparable injury to Plaintiff and Class Members as other individuals could access Plaintiff's and Class Members highly sensitive communications, messages, photographs, as well as health related information. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the class.

COUNT NINE

INTRUSION UPON SECLUSION

(Against All Defendants)

248. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

249. Plaintiff's and Class Members' Private Information is and always has been private and confidential.

1 250. Plaintiff and Class Members have and had reasonable expectations of
2 privacy in their student records, their provided PII and PHI.

3 251. The reasonableness of such expectation of privacy is supported by the
4 highly sensitive nature of the records, as well as Defendants' position in power and
5 duty to monitor Plaintiff's and Class Members' collected information.

6 252. Dissemination of Plaintiff's and Class Members' Private Information is
7 not of a legitimate public concern; publication to third parties of their Private
8 Information would be, is and will continue to be, offensive to Plaintiff, Class
9 Members, and other reasonable people.

10 253. By failing to keep Plaintiff's and Class Members' Private Information
11 secure, and disclosing Private Information to unauthorized parties for unauthorized
12 use, Defendant Keffer and the University Defendants unlawfully invaded and
13 intruded upon Plaintiff's and Class Members' privacy right to seclusion.

14 254. Defendant Keffer and the University Defendants' wrongful actions
15 and/or inaction constituted, and continue to constitute, an invasion of Plaintiff's and
16 Class Members' privacy by publicly disclosing their Private Information when they
17 allowed Defendant Weiss to exfiltrate large amounts of Private Information regarding
18 student athletes at the University as well as other institutions.

19 255. Defendant Weiss also directly invaded the privacy of Plaintiff and the
20 Class Members when he exfiltrated large amounts of data from the computer systems
21 of Keffer and the University Defendants as well as hacking into the personal accounts
22 of thousands of students, student athletes, and alumni.

23 256. Defendant Weiss' intrusions were substantial and would be highly
24 offensive to a reasonable person, constituting an egregious breach of social norms.

25 257. Plaintiff and the Class Members were, and continue to be, harmed as a
26 direct and proximate result of the Defendants' invasion of their privacy by publicly
27 disclosing their Private Information, for which they suffered loss.
28

1 Personal Information Protection Act, Cal. Bus. & Prof. Code 225841 *et seq.* (Ch. 22.2,
2 Div. 8), California Information Practices Act (“IPA”), Cal. Civ. Code 1798 *et seq.*,
3 Health Information Portability and Accountability Act, and California Confidentiality
4 of Medical Information Act (Cal. Civ. Code 56).

5 264. None of the Defendants, however, ensured that their computer systems
6 were secure and failed to adequately protect the users of their systems, including
7 students.

8 265. The University Defendants and Keffer knew the sensitivity of the
9 information kept on its system but failed to ensure that it was secure.

10 266. For the above reasons and others, the University Defendants and Keffer
11 breached the duty of reasonable care to Plaintiff and the Class Members.

12 267. Furthermore, University Defendants are also liable for actions of its
13 employees and vendors – including Keffer – under vicarious liability. Each
14 University Defendant had a duty to monitor, supervise, control, and otherwise provide
15 the necessary oversight to safeguard the PII and PHI of their students that they
16 collected, stored, and processed on their and Keffer’s systems. At all material times
17 herein, University Defendants had control or the right to control the actions of Keffer,
18 and yet they failed to take any action to ensure that the PII and PHI of their students
19 was protected.

20 268. As a direct and proximate result of the University Defendants and
21 Keffer’s actions and omissions, Plaintiff and the Class Members had their personal
22 information targeted, stolen, and viewed without their knowledge or permission.

23 269. As a direct and proximate result of the University Defendants and
24 Keffer’s general negligence, Plaintiff suffered economic and non-economic damages.

25 270. Plaintiff, individually, on behalf of the Class members, seeks all monetary
26 and non-monetary relief allowed by law, including actual damages, statutory
27 damages, punitive damages, preliminary and other equitable or declaratory relief, and
28 attorneys’ fees and costs.

COUNT ELEVEN

STATUTORY CIVIL LARCENY

(Against Weiss)

271. Plaintiff, individually and on behalf of the Class Members, herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

272. Section 496(a) of the California Penal Code specifically prohibits the obtaining of property “in any manner constituting theft.”

273. Section 484 of the California Penal Code defines “theft” to include any actions that “steal, take, carry, lead, or drive away the personal property of another”.

274. Plaintiff and the Class Members Private Information, including their personal photos and private communications, were their personal property.

275. Weiss stole, and/or fraudulently appropriated Plaintiff’s and the Class Members’ personal information without their consent.

276. Plaintiff and the Class Members suffered actual damages as a result of Weiss’ theft of their personal property to which he was not entitled.

277. Section 496(c) of the California Penal Code allows any person “injured by a violation” of this section to “bring an action for three times the amount of actual damages, if any, sustained by the Plaintiff, costs of suit, and reasonable attorney’s fees.”

278. Plaintiff, individually, and on behalf of the Class Members, seeks all monetary and non-monetary relief allowed by law, including treble damages, and attorneys’ fees and costs.

COUNT TWELVE

CALIFORNIA INFORMATION PRACTICES ACT, CAL. CIV. CODE §

1798, et seq.

(Against University Defendants)

279. Plaintiff, individually and on behalf of the Class Members, herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

280. The California Information Practices Act (“IPA”) requires that agencies report unauthorized disclosure of personal information “in the most expedient time possible and without unreasonable delay.” Cal. Civ. Code § 1798.29.

281. The University Defendants are bound to this duty as they are both an “agency” and more specifically, under Cal. Gov. Code § 1798.3.

282. The Legislature imposed this duty to give notice “in order to protect the privacy of individuals,” stating that “is it is necessary that the maintenance and dissemination of personal information be subject to strict limits.” Plaintiff and the Class Members suffered the exact harm this statute was meant to avoid, as their “right to privacy is a personal and fundamental right” that was infringed by the University Defendants’ negligent notice procedures. Cal. Civ. Code § 1798.1.

283. Plaintiff, individually, on behalf of the Class Members, seeks all monetary and non-monetary relief allowed by law, including treble damages, and attorneys’ fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Proposed Classes defined herein, respectfully request:

- A. Enter a judgment encompassing the relief requested above, plus significant compensatory damages exceeding \$5,000,000.00 together with costs, interest and attorney fees, against Defendants, and such other relief to which they are entitled;
- B. An order certifying the proposed Class and Subclasses; designating Plaintiff as the named representative of the respective Class Members; and appointing her counsel as Class Counsel;
- C. All such equitable relief as the Court deems proper and just, including but not limited to, declaratory relief;
- D. Enter judgment in favor of Plaintiff and against Defendant Weiss for treble the amount of their actual damages resulting from Weiss’ theft of

their personal property, plus attorney's fees and costs for violation of California Penal Code §§ 484 and 496;

E. Award Plaintiff costs, attorney fees as well as interest from the date of Judgment until paid; and

F. Grant such further relief as is agreeable to equity and good conscience.

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all triable issues.

DATED: April 23, 2025

Respectfully Submitted,
CLARKSON LAW FIRM, P.C.

/s/ Yana Hart

Ryan Clarkson, Esq.
Yana Hart, Esq.
Bryan P. Thompson, Esq.
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050

SOMMERS SCHWARTZ, P.C.

Lisa M. Esser (P70628)
Richard L. Groffsky (P32992)
Jason J. Thompson (P47184)
Matthew G. Curtis (P37999)
One Towne Square, 17th Floor
Southfield, MI 48076
Tel: (248) 355-0300

**PITT MCGEHEE PALMER
BONANNI & RIVERS, P.C.**

Megan Bonanni (P52079)
Kevin M. Carlson (P67704)
Beth M. Rivers (P33614)
Danielle Y. Canepa (P82237)
117 W. Fourth Street, Suite 200
Royal Oak, MI 48067
Tel: (248) 398-9800

*Counsel for Plaintiff and
the Proposed Class*

[Query](#)[Reports](#)[Utilities](#)[Help](#)[Log Out](#)

18BD

**U.S. District Court
North Carolina Middle District (NCMD)
CIVIL DOCKET FOR CASE #: 1:25-cv-00303-CCE-JLW**

DOE 1, et al v. HIGH POINT UNIVERSITY, et al
Assigned to: Chief/Senior Distric CATHERINE C. EAGLES
Referred to: MAG/JUDGE JOE L. WEBSTER
Cause: 28:1331 Fed. Question

Date Filed: 04/23/2025
Jury Demand: Plaintiff
Nature of Suit: 890 Other Statutory Actions
Jurisdiction: Federal Question

Plaintiff**JANE DOE 1**

*on behalf of themselves and others similarly
situated*

represented by **JAMES J. MILLS**
BURNS DAY & PRESNELL, P.A.
POB 10867
RALEIGH, NC 27605
919-782-1441
Fax: 919-782-2311
Email: jmills@bdppa.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

KEVIN CARLSON
PITT MCGEHEE PALMER BONANNI &
RIVERS PC
117 WEST FOURTH STREET
SUITE 200
ROYAL OAK, MI 48067
248-398-9800
Fax: 248-298-7996
Email: kcarlson@pittlawpc.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

MEGAN A BONANNI
PITT MCGEHEE PALMER BONANNI &
RIVERS
117 W. FOURTH STREET
SUITE 200
ROYAL OAK, MI 48067
248-398-9800
Fax: 248-268-7996
Email: mbonanni@pittlawpc.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

JASON THOMPSON
SOMMERS SCHWARTZ, P.C.
ONE TOWNE SQUARE

SUITE 1700
Southfield, MI 48076
248-355-0300
Email: jthompson@sommerspc.com
ATTORNEY TO BE NOTICED

LISA MICHELLE ESSER
SOMMERS SCHWARTZ, P.C.
ONE TOWNE SQUARE
STE 1700
SOUTHFIELD, MI 48076
248-355-0300
Email: lesser@sommerspc.com
ATTORNEY TO BE NOTICED

MATTHEW G CURTIS
SOMMERS SCHWARTZ, PC
ONE TOWNE SQUARE
STE 17TH FLOOR
SOUTHFIELD, MI 48076
248-746-4038
Fax: 248-936-2124
Email: mcurtis@sommerspc.com
ATTORNEY TO BE NOTICED

RICHARD GROFFSKY
SOMMERS SCHWARTZ, P.C.
ONE TOWNE CENTER
STE 1700
SOUTHFIELD, MI 48076
248-746-4028
Email: rgroffsky@gmail.com
ATTORNEY TO BE NOTICED

Plaintiff

JANE DOE 2

*on behalf of themselves and others similarly
situated*

represented by **JAMES J. MILLS**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

KEVIN CARLSON
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

MEGAN A BONANNI
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

JASON THOMPSON
(See above for address)
ATTORNEY TO BE NOTICED

LISA MICHELLE ESSER

(See above for address)

*ATTORNEY TO BE NOTICED***MATTHEW G CURTIS**

(See above for address)

*ATTORNEY TO BE NOTICED***RICHARD GROFFSKY**

(See above for address)

ATTORNEY TO BE NOTICED

V.

Defendant**HIGH POINT UNIVERSITY****Defendant****MATTHEW WEISS****Defendant****KEFFER DEVELOPMENT SERVICES,
LLC.**

Date Filed	#	Docket Text
04/23/2025	<u>1</u>	PLAINTIFFS' CLASS ACTION COMPLAINT AND JURY DEMAND against HIGH POINT UNIVERSITY, Keefer Development Services LLC, Matthew Weiss (Filing fee \$ 405 receipt number ANCMDC-4073111.), filed by JANE DOES. (Attachments: # <u>1</u> Exhibit 1, # <u>2</u> Exhibit 2)(MILLS, JAMES) Modified on 4/25/2025 to match title of document. (sh) (Entered: 04/23/2025)
04/24/2025		Case ASSIGNED to Chief/Senior District Judge CATHERINE C. EAGLES and MAG/JUDGE JOE L. WEBSTER. (lg) (Entered: 04/24/2025)
04/29/2025	<u>2</u>	NOTICE of Special Appearance by attorney MEGAN A BONANNI on behalf of All Plaintiffs Megan A Bonanni (Filing fee \$ 25 receipt number ANCMDC-4077711.) (BONANNI, MEGAN) (Entered: 04/29/2025)
05/01/2025	<u>3</u>	MOTION to Appoint Counsel (<i>Interim Class</i>) by JANE DOE 1, JANE DOE 2. (Attachments: # <u>1</u> Exhibit 1 - Weiss Indictment, # <u>2</u> Exhibit 2 - IL Complaint, # <u>3</u> Exhibit 3 - CA Complaint, # <u>4</u> Exhibit 4 - MD Complaint, # <u>5</u> Exhibit 5 - NC Complaint, # <u>6</u> Exhibit 6 - CMC Order, # <u>7</u> Exhibit 7 - Joint Submission, # <u>8</u> Exhibit 8 - Motion for CMC, # <u>9</u> Exhibit 9 - S2 Leadership Bios, # <u>10</u> Exhibit 10 - Pitt Leadership Bios, # <u>11</u> Exhibit 11 - proposed Order)(MILLS, JAMES) (Entered: 05/01/2025)
05/02/2025	<u>4</u>	NOTICE of Special Appearance by attorney KEVIN CARLSON on behalf of All Plaintiffs Kevin M Carlson (Filing fee \$ 25 receipt number ANCMDC-4079958.) (CARLSON, KEVIN) (Entered: 05/02/2025)
05/05/2025	<u>5</u>	MEMORANDUM in Support of Plaintiffs' <u>3</u> MOTION to Appoint Counsel (<i>Interim Class</i>). (MILLS, JAMES) Modified on 5/5/2025 to set out pleading title. (lg) (Additional attachment(s) added on 5/5/2025: # <u>1</u> Exhibit 1 - Weiss Indictment, # <u>2</u> Exhibit 2 - IL Complaint, # <u>3</u> Exhibit 3 - CA Complaint, # <u>4</u> Exhibit 4 - MD Complaint, # <u>5</u> Exhibit 5 -

		NC Complaint, # 6 Exhibit 6 - CMC Order, # 7 Exhibit 7 - Joint Submission, # 8 Exhibit 8 - Motion for CMC, # 9 Exhibit 9 - S2 Leadership Bios, # 10 Exhibit 10 - Pitt Leadership Bios, # 11 Exhibit 11 - Proposed Order) (lg). (Entered: 05/05/2025)
05/06/2025		Motions Submitted: 3 MOTION to Appoint Counsel (<i>Interim Class</i>) to Chief/Senior District Judge CATHERINE C. EAGLES (rw) (Entered: 05/06/2025)
05/06/2025		Motions No Longer Submitted 3 MOTION to Appoint Counsel (<i>Interim Class</i>) to Judge Eagles (rw) (Entered: 05/06/2025)
05/07/2025	6	WAIVER OF SERVICE of SUMMONS by JANE DOE 2, JANE DOE 1. KEFFER DEVELOPMENT SERVICES, LLC. waiver sent on 5/5/2025, answer due 7/7/2025. (MILLS, JAMES) (Entered: 05/07/2025)
05/08/2025	7	STANDARD ORDER for civil cases proceeding before Chief/Senior District Judge CATHERINE C. EAGLES. (rw) (Entered: 05/08/2025)
05/08/2025	8	NOTICE of Special Appearance by attorney LISA MICHELLE ESSER on behalf of Plaintiffs JANE DOE 1, JANE DOE 2 (Filing fee \$ 25 receipt number ANCMDC-4083642.) (ESSER, LISA) (Entered: 05/08/2025)
05/08/2025	9	NOTICE of Special Appearance by attorney JASON THOMPSON on behalf of Plaintiffs JANE DOE 1, JANE DOE 2 (Filing fee \$ 25 receipt number ANCMDC-4083945.) (THOMPSON, JASON) (Entered: 05/08/2025)
05/09/2025	10	Summons Issued as to HIGH POINT UNIVERSITY, MATTHEW WEISS. (Attachments: # 1 Summons - Weiss) (sh) (Entered: 05/09/2025)
05/09/2025	11	Notice of Right to Consent. Counsel shall serve the attached form on all parties. (Attachments: # 1 Consent Form) (sh) (Entered: 05/09/2025)
05/19/2025	12	NOTICE of Special Appearance by attorney RICHARD GROFFSKY on behalf of Plaintiffs JANE DOE 1, JANE DOE 2 (Filing fee \$ 25 receipt number ANCMDC-4091492.) (GROFFSKY, RICHARD) (Entered: 05/19/2025)
06/02/2025	13	SUMMONS Returned Executed by JANE DOE 2, JANE DOE 1 as to HIGH POINT UNIVERSITY served on 5/30/2025, answer due 6/20/2025. on Personal Service Steven Calloway Registered Agent of High Point University (ESSER, LISA) (Entered: 06/02/2025)
06/04/2025	14	NOTICE of Special Appearance by attorney MATTHEW G CURTIS on behalf of Plaintiffs JANE DOE 1, JANE DOE 2 (Filing fee \$ 25 receipt number ANCMDC-4102438.) (CURTIS, MATTHEW) (Entered: 06/04/2025)

PACER Service Center			
Transaction Receipt			
06/05/2025 16:20:58			
PACER Login:	ThomaKingking	Client Code:	
Description:	Docket Report	Search Criteria:	1:25-cv-00303-CCE-JLW
Billable Pages:	4	Cost:	0.40

**IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA
CASE NO: 25-CV-303**

JANE DOES 1 and 2 , on behalf of themselves)	
and others similarly situated,)	
)	
Plaintiffs,)	
)	
v.)	
)	
MATTHEW WEISS, HIGH POINT UNIVERSITY,)	
and KEFFER DEVELOPMENT SERVICES, LLC.)	
)	
Defendants.)	

PLAINTIFFS' CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiffs JANE DOES 1 AND 2, through their attorneys, Sommers Schwartz, P.C., Pitt McGehee Palmer Bonanni & Rivers, P.C., and Burns, Day & Presnell, PA, for their Complaint against MATTHEW WEISS, HIGH POINT UNIVERSITY, and KEFFER DEVELOPMENT SERVICES, LLC, state as follows:

I. INTRODUCTION

Students and alumni connected to High Point University from 2015 to 2023—many of them student-athletes—have been subjected to a deeply troubling and unlawful breach of privacy, stemming from the actions of former University of Michigan and Baltimore Ravens football coach Matthew Weiss, whose gross and despicable violations of their privacy were facilitated by institutional negligence. This class action lawsuit, filed against Matthew Weiss, High Point University, and Keffer Development Services, LLC, seeks justice for the unauthorized access and misuse of personal information—an abuse so severe that High Point University students and student-athletes are now receiving formal notification from the U.S. Department of Justice that their private information, including intimate photos and videos, have been exposed, including

Plaintiffs Jane Does 1 and 2. This action is brought to hold the Defendants accountable for failing to protect their students from foreseeable harm.

II. PARTIES

1. Plaintiff Jane Doe 1 was a student athlete at High Point University between 2006-2010 and was a member of the Cheerleading Team.

2. Plaintiff Jane Doe 1 is domiciled in the state of North Carolina in the City of Charlotte.

3. On or about March 25, 2025, Plaintiff Jane Doe 1 received notice from the United States Department of Justice Victim Notification System that she was identified as a victim in the criminal case against University of Michigan's Coach Weiss: *United States v. Defendant(s) Matthew Weiss*.¹

4. Plaintiff Jane Doe 2 was a student at High Point University between 2011-2016.

5. Plaintiff Jane Doe 2 is domiciled in the state of New York in the City of New York.

6. On or about March 26, 2025, Plaintiff Jane Doe 2 received notice from the United States Department of Justice Victim Notification System that she was identified as a victim in the criminal case against University of Michigan's Coach Weiss: *United States v. Defendant(s) Matthew Weiss*.²

7. Defendant High Point University ("University") is a private university in High Point, North Carolina (Guilford County).

8. High Point University enrolls approximately 5,781 undergraduate and graduate students.

¹ Jane Doe 1's DOJ Data Breach Notice is attached hereto as **Exhibit 1**.

² Jane Doe 2's DOJ Data Breach Notice is attached hereto as **Exhibit 2**.

9. High Point University is a member of the National Collegiate Athletic Association (NCAA), with student athletes competing in 16 intercollegiate sports at the Division 1 level.

10. Defendant Keffer Development Services, LLC, (“Keffer”) is a Pennsylvania limited liability company in Grove City, PA, that has continuously and systemically conducted business in North Carolina by directly providing services to residents and entities within the State of North Carolina, including its business contacts with High Point University in High Point, North Carolina, thereby availing itself of protections of the law of the State of North Carolina.

11. Defendant Keffer is a technology and data vendor operating an electronic medical record and student athlete training system, which stored the personal identifying information (“PII”) and personal health information (“PHI”) of Plaintiffs and Class Members across the country.

12. Any wrongful conduct and legal violations committed by Defendant Keffer that are subsequently outlined in this Complaint occurred specifically with respect to the Plaintiffs during the time of the incident alleged in this Complaint.

13. Matthew Weiss (“Weiss”) is an individual residing in the State of Michigan, who had contacts with the State of North Carolina in that he conducted illegal activity in the State of North Carolina, by hacking into the personal property of Plaintiffs and putative Class Members of the State of North Carolina during the applicable time period at issue in this Complaint and said activities from which this Complaint arises.

14. On March 20, 2025, Defendant Weiss was indicted on 24 counts of unauthorized access to computers and aggravated identity theft by the U.S. Attorney for the Eastern District of Michigan.

III. JURISDICTION AND VENUE

15. Jurisdiction is proper in this Court under 28 U.S.C. §§ 1331 and 1367 as this matter involves a claim under the Stored Communications Act, 18 U.S.C. § 2701(a) *et seq.*; the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; Title IX, 20 U.S.C. § 1681(A) *et seq.*; 42 U.S.C. § 1983; the Fourth Amendment of the U.S. Constitution; and the Fourteenth Amendment of the U.S. Constitution, and this Court has supplemental jurisdiction of all additional causes of action alleged in this Complaint pursuant to 28 U.S.C. §1367(a).

16. This Court also has subject matter jurisdiction pursuant to 28 U.S.C. §1332(d) under the Class Action Fairness Act (“CAFA”) as a class action lawsuit in which the amount in controversy exceeds \$5,000,000.00, there are more than one-hundred putative Class Members, and the majority of the putative Class Members are citizens of a state different than the state of which Defendants are citizens.

17. The Court has personal jurisdiction over Defendants named in this action because Defendant University is located and created under the laws of the State of North Carolina, and Defendant Weiss had minimum contacts with the State of North Carolina as set forth above, thus purposefully availing himself of the privilege of conducting activities in the State of North Carolina. Defendant Keffer conducts business in the State of North Carolina and has availed itself of the protections of North Carolina state law. The claims at issue in this case arise out of Defendants’ purposeful contacts with and business activities in the State of North Carolina.

18. Venue is appropriate in this District Court under 28 U.S.C. §1391(b) since a substantial part of the events or omissions giving rise to these claims occurred within this District.

19. Plaintiffs’ injuries are redressable by monetary compensation, and all alleged injuries of Plaintiffs and Class Members can be traced to Defendants’ conduct.

IV. COMMON ALLEGATIONS

A. WEISS’S DATA BREACH AND CYBER SEXUAL ASSAULT OF THOUSANDS OF STUDENTS FOR NEARLY A DECADE AND THE ROLE DEFENDANT KEFFER AND UNIVERSITY PLAYED IN HIS SCHEME

20. Plaintiffs bring this class action against Defendants University and Keffer for their failure to properly secure the highly sensitive personally identifiable information (“PII”) and protected health information (“PHI”) of more than 150,000 students, including [Plaintiffs, which was targeted, accessed, and exfiltrated by former University of Michigan and Baltimore Ravens coach and sexual predator Matthew Weiss, over the course of nearly a decade.

21. Between 2015 and January 2023, Defendant Weiss gained unauthorized access to both student databases and student-athlete databases of more than 100 colleges and universities, some of which were maintained by Defendant Keffer, a third-party vendor contracted by these colleges and universities.

22. Upon information and belief, Defendant High Point University contracted with Defendant Keffer.

23. After gaining access to these databases, Weiss downloaded the PII and PHI of more than 150,000 athletes.

24. Using the information that Weiss obtained from the student and student-athlete databases and his own research, Weiss was able to obtain access to the social media, email, and/or cloud storage accounts of more than 2,000 students. Defendant Weiss also illegally obtained access to the social media, email, and/or cloud storage accounts of more than 1,300 additional students and/or alumni from universities and colleges across the country. Once Weiss obtained access to these accounts, he downloaded personal, intimate digital photographs and videos that were never intended to be shared beyond intimate partners.

25. Defendant Weiss primarily targeted female college athletes. He researched and targeted these women based on their school affiliation, athletic history, and physical characteristics.

26. Through this scheme, unknown to students and student athletes, Defendant Weiss downloaded intimate digital photographs and videos.

27. This scheme appears to be the largest cyber sexual assault of student athletes in U.S. history.

28. The data breach and cyber sexual assault of over 150,000 students from university and college databases, including athletic databases maintained by Keffer, and the targeted exfiltration of intimate, personal, digital photographs and videos of 3,300 students and athletes, continued for nearly a decade because Defendant High Point University and Defendant Keffer failed to prevent, detect, or stop Weiss from accessing those databases without and in excess of any authorization.

29. In at least several instances, Defendant Weiss exploited vulnerabilities in universities' account authorization processes to gain access to the accounts of students or alumni. Weiss then leveraged his access to these accounts to gain access to other social media, email, and/or cloud storage accounts.

30. That level of access through that number of accounts is an egregious and grossly negligent failure of data security on its face, as no institution with reasonable data security would allow such a breach over an eight-year period.

31. In March 2025, Matthew Weiss was charged in a 24-count indictment alleging 14 counts of unauthorized access to computers and 10 counts of aggravated identity theft, by the U.S.

Attorney for the Eastern District of Michigan, for Weiss's perpetration of the cyber sexual assaults and data breach.

B. DEFENDANT KEFFER AND ITS "ATHLETIC TRAINER SYSTEM"

32. Defendant Keffer is a software development vendor that developed an electronic medical record system known as "The Athletic Trainer System," which is used by many schools, colleges and universities across the United States.³

33. Defendant Keffer was founded in 1994 and currently collaborates with over 600 clients across 48 states and internationally.⁴ Defendant Keffer advertises that it currently serves over 6,500 schools, clinics, and other organizations with over 27,000 users and 2 million athletes.⁵

34. Upon information and belief, among the universities served by Keffer are Defendant University and Jane Does 1 and 2's alma mater.

35. Keffer represents that its Athletic Trainer System tool was "designed with athletic trainers for athletic trainers," and is designed to store personal identifying information and personal health information belonging to students including their treatment histories, diagnoses, injuries, photos, and personal details, like height and weight, mental health information, and demographic information.⁶

36. In Keffer's FAQ, it boasts that: "Keffer Development hosts all databases in our SSAE-16, SOC II and FedRamp certified data center" and that "Information security is a high priority in our company."⁷ Keffer further claims that "On top of our Data Center being FedRamp

³ https://www.athletictrainersystem.com/pdf_files/Athlete_Info.pdf.

⁴ <https://www.athletictrainersystem.com/CompanyHistory.aspx>

⁵ <https://www.athletictrainersystem.com/Default.aspx>

⁶ See <https://www.athletictrainersystem.com/DemoRequest.aspx>

⁷ https://www.athletictrainersystem.com/pdf_Files/ATS_FAQ.pdf

Certified, ATS is also HIPAA and FERPA compliant. We utilize a company called Compliance Helper to ensure we maintain HIPAA and FERPA compliance.”⁸

37. In Keffer’s Privacy Policy, it acknowledges that it has obligations as a “business associate” under HIPAA: “To the extent that KDS [Keffer] receives or maintains patient medical information in the course of providing the Clinical EMR, that information is secured, used and disclosed only in accordance with KDS’ legal obligations as a “business associate” under HIPAA.”⁹

38. Keffer’s Privacy Policy further states: “KDS understands that storing our data in a secure manner is essential. KDS stores PII, PHI and other data using industry-standard physical, technical and administrative safeguards to secure data against foreseeable risks, such as unauthorized use, access, disclosure, destruction or modification. Please note, however, that while KDS has endeavored to create a secure and reliable website for users, the confidentiality of any communication or material transmitted to/from the Website or via e-mail cannot be guaranteed.”¹⁰

39. Despite recognizing these obligations, Keffer failed to implement basic, industry standard systems to protect students’ – including Jane Does 1 and 2’s - personal identifying information and protected health information.

40. As an example, while Keffer maintained the option to incorporate two-factor authentication to access its Athletic Trainer System applications, it did not require that institutions and users do so.¹¹ A two-factor basic security measure that requires an additional layer of authentication on top of a login credential, such as a code sent via text message or email – and

⁸ *Id.*

⁹ https://www.athletictrainersystem.com/pdf_Files/ATS_Privacy_Policy.pdf

¹⁰ *Id.*

¹¹ https://www.athletictrainersystem.com/pdf_Files/ATS_FAQ.pdf

critically, would have prevented Defendant Weiss from gaining access to student protected health information with only the access credentials belonging to other administrators and users.

41. Defendants knew that Keffer did not require institutions and users to use two-factor authorization to access the private information and communications accessible through its system, including information maintained in the Defendant High Point University's facilities, and thus knowingly and deliberately permitted Plaintiffs' confidential information and communications to be accessed, shared, and divulged without authorization from Plaintiffs.

42. Recent actions by the FTC underscore the gross negligence and failings of Keffer and Defendant High Point University in failing to ensure that the Athletic Trainer System was configured to default to two-factor or multi-factor authentication for access to its systems containing personal identifying information and protected health information. In February 2023, the FTC published an article titled, *Security Principles: Addressing Underlying Causes of Risk in Complex Systems*. The article highlighted the importance of multi-factor authentication (MFA), stating: "Multi-factor authentication is widely regarded as a critical security practice because it means a compromised password alone is not enough to take over someone's account."¹²

43. Additionally, the FTC's enforcement actions over the past five years further emphasize the critical and fundamental role MFA plays in an effective data security system, where the FTC has repeatedly obtained MFA as a form of injunctive relief in data security enforcement actions.¹³

¹²<https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems>

¹³ E.g., *In re: Equifax* (July 2019), <https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach>; *In re Drizly* (Oct. 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/10/drizly-pay-5-million-part-settlement-ftc-cfpb-states-related-2021-data-breach>

44. Keffer also lacked any effective data auditing program to measure the download activity from its system, which would have allowed it to detect the massive, years-long data breach on its systems by Defendant Weiss and the resulting cyber sexual assault on Plaintiffs Jane Does 1 and 2 and those Class Members similarly situated.

45. Both Keffer and Defendant High Point University had a responsibility and duty to protect the private data of students and student athletes stored within their databases and to have mechanisms in place to prevent such a gross invasion of privacy as what occurred in this case.

46. The risk of identity theft and breaches of security to access users' private, personal, and confidential information is foreseeable within the University and Keffer's information technology systems, and the University and Keffer are well aware of the foreseeable risks of breaches, such as those alleged in this case, that are likely to occur if their practices in detecting, preventing, and mitigating such breaches are substandard.

C. DEFENDANT UNIVERSITY'S FAILURE TO SAFEGUARD ITS STUDENTS' PRIVATE INFORMATION FOR NEARLY A DECADE

47. Defendant High Point University is an established high-level educational institution, with a diverse athletic program, enrolling over 5,000 students and student athletes who participate in 16 different sports at the NCAA Division 1 level.

48. In maintaining its academics and athletics department, High Point University provides its students with medical care and its student athletes with athletic trainers.

49. The University had a responsibility and duty to oversee the University's operations, policies and procedures, and to care for and protect the University's students.

[releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million.](#)

50. The University was required to ensure that students, such as Jane Does 1 and 2, were not exposed to sexual predators who would invade their privacy.

51. The University failed in this duty by failing to take any reasonable action to prevent the harm caused to Jane Does 1 and 2 and other Class Members as alleged in this Complaint.

52. This prolific and egregious breach and violation was entirely preventable by the University and Keffer. As noted in a criminal complaint filed by the U.S. Attorney for the Eastern District of Michigan, Defendant Weiss breached University and Keffer's systems and the systems of colleges and universities across this nation by exploiting passwords and other vulnerabilities in the systems and authentication processes of Keffer and these universities. On information and belief, neither the University nor Keffer required that its employees or students implement safeguards like multi-factor authentication to access accounts, a standard practice for all entities collecting personal identifying information, especially medical data and PHI (protected health information).

53. The breach and cyber assaults were a direct result of Defendant High Point University's and Keffer's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Jane Does 1 and 2 and Class Members PII and PHI, leaving the most sensitive and personal information of students, like Jane Does 1 and 2, vulnerable to exploitation by malicious predators like Defendant Weiss.

54. Defendant High Point University was grossly negligent on two fronts: (1) in its hiring and oversight of Defendant Keffer and its entrusting of students' PII and PHI in the care of Defendant Keffer, and (2) in its maintenance, oversight and security of its own internal databases of those internal systems to protect student PII and PHI.

55. The University took no reasonable actions to prevent this access despite its duties to students and has taken no reasonable actions to notify or rectify harm to the victims of Matthew Weiss's misconduct and predation.

56. Thousands of students remain at risk because the University and Keffer have failed to undertake any reasonable review of how Jane Does 1 and 2's private and personal information is stored, maintained, and who can access such information, and from where.

57. To this day, the University has not formally informed Class Members impacted by Weiss's cyber sexual assault and misconduct.

D. HIGH POINT UNIVERSITY WAS NEGLIGENT IN HIRING/CONTRACTING WITH DEFENDANT KEFFER AND IN ENTRUSTING STUDENTS PII AND PHI TO KEFFER

58. Defendant High Point University provided its students and student athletes medical treatment, including from athletic trainer employees of the University.

59. To facilitate that treatment, the University utilized its own database and additionally contracted with Keffer to use its Athletic Training System application, which required that student athletes provide the University and Keffer with sensitive PII and PHI.

60. When collecting that information, the University, like Keffer, accepted an obligation to protect that information under contract and statutory principles, including as a "business associate" under HIPAA.

61. Jane Does 1 and 2 and others similar to them entrusted that the University and Keffer would safeguard their private information and ensure the security and confidentiality of their data.

62. The University and Keffer had, and continue to have, a duty to protect Jane Does 1 and 2 and to take appropriate security measures to protect private, personal, medical and intimate information, communications, and images.

63. The University knowingly and deliberately permitted access to and divulging of Plaintiffs' stored communications through its database and Keffer and failed to take reasonable action to ensure that protected the privacy of the sensitive information of Jane Does 1 and 2 and others like them.

64. Upon information and belief, the University failed to properly evaluate its own database and failed to implement protocols and failed to adequately monitor or establish safeguards with the students and their private information to ensure they carried out their duties to safeguard and protect the private information of their students entrusted to them.

65. Upon information and belief, the University failed to investigate Keffer and Keffer's protocols, and failed to adequately monitor or establish safeguards for Keffer's work with the students and their private information to ensure they carried out their duties to safeguard and protect the private information of their students entrusted to them.

66. The University was negligent and/or reckless in failing to ensure that media and other private, personal and sensitive information, including but not limited to that of Jane Does 1 and 2 was securely protected, as the University was entrusted to do.

67. The University failed to implement the security measures necessary to protect their students' PII and PHI, including failing to train staff and employees on securing credentials, requiring multi-or-two-factor authentication to use their database and Keffer's Athletic Trainer System, overseeing third-party vendors like Keffer, in which the University entrusted students' sensitive PII and PHI and monitoring and auditing access to student files and private information.

68. In other words, the University not only failed to ensure it had implemented sufficient security protocols and procedures across its own systems and staff, but also the University failed to ensure Keffer had adequate security measures in place to protect its students' PII and PHI from theft and misuse.

69. The University lacked adequate training programs to detect and stop breaches like those caused by Defendant Weiss.

70. The University and Keffer failed to implement reasonable protective measures to detect Weiss' irregular activity and trespassing, including but not limited to, appropriate authentication tools, behavioral analytics, anomaly detection, machine learning, and real-time monitoring of user activity, looking for deviations from established patterns and suspicious actions like unusual login attempts or access to sensitive data, any of which would have prevented Weiss' improper access to private student information.

71. Because Keffer and the University failed to implement basic, industry standard security measures, together these Defendants allowed an alleged sexual predator, ex-football coach Matthew Weiss, to access students', and in particular female student athletes', most sensitive information for nearly a decade.

72. All Defendants disregarded the rights of Jane Does 1 and 2 and Class Members. The University and Keffer knowingly, intentionally, willfully, recklessly and/or negligently provided access to and/or divulged Plaintiffs' private communications stored in their facilities; failed to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failed to disclose that they did not have adequately robust computer systems and security practices to safeguard private information; failed to take standard and reasonably available steps to prevent the data breach and cyber assault; failed to properly train

their staff and employees on proper security measures; failed to provide Jane Does 1 and 2 and the Class Members prompt notice of the data breach and cyber assault.

73. Defendants High Point University's and Keffer's conduct amounts to a violation of the duties they owed to Jane Does 1 and 2 under common law and state and federal statutory law, rendering them liable to Jane Does 1 and 2 and the Class Members for the harms caused by this egregious and preventable cyber sexual assault and invasion of privacy. Defendant Weiss is equally liable for the harm inflicted on Jane Does 1 and 2 and the Class Members by his intentional hacking and exfiltration of their private information under tort and statutory law.

74. Jane Does 1 and 2 and the putative Class Members are current and former students at High Point University and other affected institutions in the United States that were specifically targeted by Weiss and harmed by the violation of their privacy.

75. Jane Does 1 and 2 and the putative Class Members suffered injury as a result of Defendants' conduct. These injuries included: invasion and loss of privacy, loss of dignity, humiliation, embarrassment, and severe emotional distress.

76. Jane Does 1 and 2 seek to remedy these harms on behalf of themselves and all similarly situated individuals whose private information was accessed by Weiss.

77. Jane Does 1 and 2 seek remedies including, but not limited to, compensatory damages, nominal damages, punitive damages, and reimbursement of out-of-pocket costs. Jane Does 1 and 2 also seek injunctive and equitable relief to prevent future injury on behalf of herself and the putative Class Members.

E. JANE DOES 1 AND 2'S ALLEGATIONS

78. Plaintiff Jane Doe 1 is a former student at High Point University.

79. While in school at High Point, Jane Doe1 participated in the Cheerleading program while Defendant Weiss's data breach and cyber sexual assault was ongoing.

80. As a student athlete, Jane Doe 1 received treatment from the University's athletic trainer staff, requiring her to disclose information about her treatment, including height, weight, injuries, medications, treatment plans, and analysis on performance and recovery. To receive treatment, Jane Doe 1 was required to use the Keffer database, and the PII and PHI Jane Doe 1 disclosed was saved on the Keffer system.

81. As a student, Jane Doe 1 was required to disclose personal information to the University and was issued a university email where sensitive, personal information was stored.

82. Because Keffer and the University never implemented the security safeguards needed to protect Jane Does 1's PII and PHI, Defendant Weiss compromised the PII and PHI belonging to every student whose information was saved by the University and/or Keffer's Athletic Trainer System database, including, on information and belief, Jane Doe 1's private and personal information.

83. Plaintiff Jane Doe 2 is a former student at High Point University.

84. Jane Doe 2 was a student while Defendant Weiss's data breach and cyber sexual assault was ongoing.

85. As a student, Jane Doe 2 received treatment from the University's medical department, requiring her to disclose information about her treatment, including height, weight, injuries, medications, treatment plans, and analysis on performance and recovery. To receive treatment, Jane Doe 2 was required to use the university database, and the PII and PHI Jane Doe 2 disclosed was saved on the university system.

86. As a student, Jane Doe 2 was required to disclose personal information to the University and was issued a university email where sensitive, personal information was stored.

87. Because Keffer and the University never implemented the security safeguards needed to protect Jane Does 2's PII and PHI, Defendant Weiss compromised the PII and PHI belonging to every student whose information was saved by the University and/or Keffer's Athletic Trainer System database, including, on information and belief, Jane Doe 1's private and personal information.

88. Defendant Weiss compromised all information that was saved in the University and/or Athletic Trainer System databases, including Plaintiffs' treatment information, injury information, height, weight, and other highly sensitive information.

89. Jane Does 1 and 2 has received notice from the U.S. Department of Justice Victim Notification System that they were identified as potential victims in the federal action against Defendant Weiss.¹⁴

90. After receiving notice from the federal government that read: "If you are receiving this notification, it means that information of yours was found in possession of the defendant,"¹⁵ Jane Does 1 and 2 felt violated, deeply disturbed, humiliated, embarrassed, and extremely emotionally distressed; and are experiencing physical manifestations of the stress and anxiety caused by this egregious violation of their privacy – symptoms that are further exacerbated by the fact that Jane Does 1 and 2 still do not have a full and complete understanding of the data breach and cyber sexual assault perpetrated by Defendant Weiss.

¹⁴ See Exhibits 1 and 2.

¹⁵ *Id.*

91. This cyber sexual assault invaded Plaintiffs' privacy and has devastated them personally and emotionally, as their highly sensitive private information was stolen by an alleged predator under circumstances that were entirely preventable by Defendant University and Defendant Keffer.

92. Upon information and belief, the United States Department of Justice is in the process of notifying thousands of potential victims that their privacy was breached.

93. As a direct result of the negligence, recklessness, and misconduct of the Defendants, Jane Does 1 and 2 and those similarly situated have incurred substantial monetary and emotional damages exceeding \$5,000,000, exclusive of costs, interest, and fees.

DEFENDANTS KEFFER AND HIGH POINT UNIVERSITY
FAILED TO PROPERLY PROTECT PLAINTIFFS' AND CLASS
MEMBERS' PII AND PHI

94. Defendants Keffer and University did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted PII and PHI it was maintaining for Plaintiffs and Class Members, causing the exposure of PII and PHI for 150,000 students and former students, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for approximately 3,330 students and former students.

95. The FTC promulgated numerous guides which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

96. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal

information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.¹⁶ The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.¹⁷

97. The FTC further recommends that companies not maintain PII and PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

98. Defendants Keffer and High Point University failed to properly implement basic data security practices explained and set forth by the FTC.

99. Defendants Keffer's and High Point University's failure to employ reasonable and appropriate measures to protect against unauthorized access PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

100. A systematic, years-long breach such as the ones Defendants Keffer and High Point University experienced is also considered a breach under the HIPAA Rules because there is an unauthorized access to PHI that is not permitted under HIPAA.

¹⁶ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

¹⁷ *Id.*

101. A breach under the HIPAA Rules is defined as, “the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI.” 45 C.F.R. 164.40.

102. Data breaches are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

The presence of ransomware (or any malware) on a covered entity’s or business associate’s computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. 45 C.F.R.164.308(a)(6).¹⁸

103. Defendants Keffer’s and High Point University’s data breach was the foreseeable consequence of a combination of insufficiencies that demonstrate that Defendants Keffer and High Point University failed to comply with safeguards mandated by HIPAA.

**DEFENDANTS HIGH POINT UNIVERSITY AND KEFFER
FAILED TO COMPLY WITH INDUSTRY STANDARDS**

104. Defendants Keffer and High Point University did not utilize industry standards appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiffs and Class Members, causing the exposure of PII and PHI for approximately 150,000 students and former students, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for 3,330 students and former students.

¹⁸ *FACT SHEET: Ransomware and HIPPA*, U.S. Dept of Health and Hum. Servs., at 4 (July 11, 2016), <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>.

105. As explained by the FBI, “[p]revention is the most effective defense against cyberattacks] and it is critical to take precautions for protection.”¹⁹

106. To prevent and detect cyberattacks, including the cyberattack that resulted in this prolific data breach and cyber sexual assault, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of cyberattacks and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

¹⁹ See How to Protect Your Networks from RANSOMWARE, at 3, <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Dec. 20, 2024).

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common cyberware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.²⁰

107. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the data breach and cyber sexual assault, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the Internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . .
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it....

²⁰ *Id.* at 3-4.

- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic....²¹

108. To prevent and detect cyberattacks, including the cyberattack that resulted in the data breaches and cyber sexual assaults, Defendants Keffer and High Point University could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure Internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

²¹ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), <https://www.cisa.gov/news-events/news/protecting-against-ransomware> (last visited Feb. 20, 2025).

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].²²

109. As described above, experts studying cyber security routinely identify medical facilities as being particularly vulnerable to cyberattacks because of the value of the private information they collect and maintain.

110. Several best practices have been identified that at a minimum should be implemented by institutions such as Defendants Keffer and High Point University, including, but not limited to, the following: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

111. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and

²² See *Human-Operated Ransomware Attacks: A Preventable Disaster* (Mar 5, 2020), <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>.

routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

112. Given that Defendants Keffer and High Point University were storing the private information of 150,000 individuals combined, Defendants Keffer and High Point University could and should have implemented all of the above measures to prevent cyberattacks, along with the two-or multi-factor authentication discussed earlier in this Complaint.

113. The occurrence, scope and duration of the breach and cyber sexual assaults indicates that Defendants Keffer and High Point University failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the exposure of approximately 150,000 students' and former students' PII and PHI, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for 3,330 students and former students.

**DEFENDANTS KEFFER AND UNIVERSITY FAILED TO PROPERLY
PROTECT PII AND PHI**

114. Defendants Keffer and High Point University breached their obligations to Jane Does 1 and 2 and Class Members and were otherwise grossly negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches, cyber-attacks, hacking incidents, and ransomware attacks;
- b. Failing to adequately protect students' private information;
- c. Failing to properly monitor its own data security systems for existing or prior intrusions;
- d. Failing to test and assess the adequacy of its data security system;

- e. Failing to develop adequate training programs related to the proper handling of emails and email security practices;
- f. Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;
- g. Failing to require a data security system to ensure the confidentiality and integrity of electronic PHI its network created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- h. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- i. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);
- j. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);
- k. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- l. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- m. Failing to ensure that it was compliant with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);
- n. Failing to train all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);
- o. Failing to ensure that the electronic PHI it maintained is unusable, unreadable, or indecipherable to unauthorized individuals, as Defendants had not encrypted the electronic PHI as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” (45 C.F.R. §164.304 definition of encryption);
- p. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

q. Failing to adhere to industry standards for cybersecurity.

115. As the result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendants Keffer and High Point University negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' private, sensitive information.

116. Defendant High Point University was also grossly negligent in its failure to oversee the data security practices of third-party vendor—Keffer—in which it entrusted the sensitive private information of its students and former students.

117. Accordingly, as outlined below, Plaintiffs and Class Members have already been severely harmed by this egregious violation of their privacy by Defendant Weiss.

CLASS ALLEGATIONS

118. Plaintiffs file this lawsuit both individually and as representative of all others similarly situated pursuant to Fed. R. Civ. P. 23 on behalf of the following Class:

All students whose personal data, images, information, social media, or videos were accessed by Weiss without authorization (the "Class Members").

119. In addition, Plaintiffs believes a subclass may be appropriate for all class members who receive notice from the United States Department of Justice as to the likely violation of their privacy and rights by Weiss. Therefore, Plaintiffs plead a subclass as follows:

All students whose personal data, images, information, social media, or videos were accessed by Weiss without authorization and who received a notice letter from the United States Department of Justice as to Weiss (the "DOJ Letter Sub-Class").

120. Excluded from the Class are: (a) Defendants and any entity or division in which Defendants have a controlling interest, and their legal representatives, officers, directors, assigns, and successors; (b) the Judge to whom this case is assigned and the Judge's staff; and (c) the attorneys representing any parties to this Class Action.

121. Plaintiffs reserve the right to modify or amend the definition of the proposed class and/or sub-classes before the Court determines whether certification is appropriate.

NUMEROSITY – FED. R. CIV. P. 23(A)(1)

122. Law enforcement officials have disclosed the numbers of victims is significant and exceeds one thousand satisfying the numerosity requirement. Although the exact number of Class Members is uncertain at this time, it will certainly be ascertained through appropriate discovery, the number is great enough such that joinder is impracticable.

123. The members of the Class are so numerous and geographically disperse that individual joinder of all members is impracticable.

124. Similarly, Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

125. Class Members are readily identifiable from information and records in the possession of the federal and state authorities, the University, and Keffer.

126. Electronic records maintained by the University and Keffer can confirm the identification of Class Members.

COMMONALITY AND PREDOMINANCE – FED. R. CIV. P. 23(A)(2) AND 23(B)(3)

127. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and the other Class Members. Similar or identical violations, practices, and injuries are involved, and the burden of proof to establish violations of those rights involve uniform, objective questions of fact and law, both for the prosecution and for the defense.

128. The common questions of fact and law existing as to all Class Members predominate over questions affecting only individual class members. The evidence required to advance Plaintiffs' and Class Members' claims are the same, common to all; as is true of the evidence Defendants will likely rely upon in defense of this action. Thus, the elements of commonality and predominance are both met.

129. For example, establishing the facts of how, where, who, when, and through what means the invasions of Plaintiffs' and other Class Members occurred are identical.

130. Defendants' actions, inactions, negligence, and recklessness apply commonly to Plaintiffs and Class Members.

131. The downloads and invasions by Weiss and the improper conduct accessing private information through unsecure facilities without permission is common to all Class Members and has caused injury to the Plaintiffs and Class Members in common manners.

132. The majority of legal and factual issues of the Plaintiffs and the Class Members predominate over any individual questions, including:

- (a) Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members private information;
- (b) Whether Defendants Keffer and the University failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the hacking incident and cyber sexual assault;
- (c) Whether Defendants Keffer and the University's data security systems prior to and during the data breach and cyber sexual assault complied with applicable data security laws and regulations;
- (d) Whether Defendants Keffer's and the University's data security systems prior to and during the data breach and cyber sexual assault were consistent with industry standards;
- (e) Whether Defendants Keffer and the University owed a duty to Plaintiffs and Class Members to safeguard their private information;

- (f) Whether Defendants Keffer and the University breached their duty to Plaintiffs and Class Members to safeguard their private information;
- (g) Whether Defendant University was grossly negligent and/or negligent in its oversight of Defendant Keffer;
- (h) Whether Defendant University or Keffer knew or should have known that their data security systems and monitoring processes were deficient;
- (i) Whether Defendants Keffer and the University owed a duty to provide Plaintiffs and Class Members timely notice of the data breach and cyber sexual assaults, and whether Defendants Keffer and the University breached that duty to provide timely notice;
- (j) Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;
- (k) Whether Defendants' conduct was negligent or grossly negligent;
- (l) Whether Defendants' conduct was per se negligent;
- (m) Whether Defendants' conduct violated federal laws;
- (n) Whether Defendants' conduct violated state laws;
- (o) Whether Plaintiffs and Class Members are entitled to damages, civil penalties, and/or punitive damages; and
- (p) Other common questions of fact and law relative to this case that remain to be discovered.

133. Resolving the claims of these Class Members in a single action will provide benefit to all parties and the Court by preserving resources, avoiding potentially inconsistent results, and providing a fair and efficient manner to adjudicate the claims.

134. Predominance does not require Plaintiffs to prove an absence of individualized damage questions, or even proof of class wide damage in the aggregate. *Kuchar v. Saber Healthcare Holdings LLC*, 340 F.R.D. 115, 123 (N.D. North Carolina 2021) (finding individualized damages questions also do not defeat a predominance finding and noting “when

adjudication of questions of liability common to the class will achieve economies of time and expense, the predominance standard is generally satisfied even if damages are not provable in the aggregate.”)(citing *Hicks*, 965 F.3d at 460).

TYPICALITY – FED. R. CIV. P. 23(A)(3)

135. Plaintiffs’ claims are typical of those of other Class Members because all had their private information compromised as a result of the breach and cyber assault and Defendants’ malfeasance.

136. Plaintiffs’ claims are typical of the Class Members because they are highly similar and the same and related in timing, circumstance, and harm suffered. To be sure, there are no defenses available to Defendants that are unique to individual Plaintiffs. The injury and causes of actions are common to the Class as all arising from the same statutory and privacy interests.

137. In *Halliburton Co. v. Erica P. John Fund, Inc.*, 573 U.S. 258, 276 (2014) the Supreme Court concluded that so long as plaintiffs could show that their evidence is capable of proving the key elements to Plaintiffs’ claim on a class-wide basis, the fact that the defendants would have the opportunity at trial to rebut that presumption as to some of the plaintiffs did not raise individualized questions sufficient to defeat predominance. “That the defendant might attempt to pick off the occasional class member here or there through individualized rebuttal does not cause individual questions to predominate.” *Id.*

138. Certification of Plaintiffs’ claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

139. The need to conduct additional post certification stage discovery, such as further file review or class member surveys, to eliminate uninjured persons after trial, does not act as a *de*

facto bar to certification. *Nixon v. Anthem, Inc.*, 2021 WL 4037824, at *8 (E.D.Ky. Sept 1, 2021)(citing *Young v. Nationwide Mut. Ins. Co.*, 693 F.3d 532 at 540(6th Cir. 2021); *In re Visa Check/MasterMoney Antitrust Litig.*, 280 F.3d 124, 145 (2d Cir. 2001); *Perez v. First Am. Title Ins. Co.*, 2009 WL 2486003, at *7 (D. Ariz. Aug. 12, 2009) (“Even if it takes a substantial amount of time to review files and determine who is eligible for the [denied] discount, that work can be done through discovery.”); *Slapikas v. First Am. Title Ins. Co.*, 250 F.R.D. 232, 250 (W.D. Pa. 2008) (finding class action manageable despite First American's assertion that “no database exists easily and efficiently to make the determination that would be required for each file”).

140. Any remaining disputes on membership or class members damages can be left to a special master's decision. *Whitlock v. FSL Mgmt., LLC*, 2012 WL 3274973, at *12 (W.D. Ky., 2012), *aff'd*, 843 F.3d 1084 (6th Cir. 2016). By placing the validation of injury step at the end of the class trial process, no injured class members are left out, and at the same time, Defendants are not at risk for paying any uninjured class members.

ADEQUACY OF REPRESENTATION – FED. R. CIV. P. 23(A)(4)

141. Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no interests that are in conflict with those of the Class Members. In addition, they have retained counsel competent and experienced in complex class action litigation, and they will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiffs and their counsel.

SUPERIORITY OF CLASS TREATMENT – FED. R. CIV. P. 23(B)(3)

142. The class action is superior to any other available procedures for the fair and efficient adjudication of these claims, and no unusual difficulties are likely to be encountered in the management of this class action.

143. The superiority analysis required to certify a class is designed to achieve economies of time, effort and expense, and to promote uniformity of decisions as to persons similarly placed, without sacrificing procedural fairness or bringing about other undesirable results.

144. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable.

145. It would be an unnecessary burden upon the court system to require these individual Class Members to institute separate actions. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

146. Pursuing this matter as a class action is superior to individual actions because:

- (a) Separate actions by Class Members could lead to inconsistent or varying adjudications that would confront Defendants with potentially incompatible standards of conduct;
- (b) Many victims will not come forward without a certified class;
- (c) Final equitable relief will be appropriate with respect to the entire Class as a whole for monitoring, protection, therapy and other equitable forms of relief that may be provided;
- (d) This action is manageable as a class action and would be impractical to adjudicate any other way;
- (e) Absent the class action, individual Class Members may not know if their privacy was invaded; where such images are currently being stored, or are accessible by others; and their injuries are likely to go unaddressed and unremedied; and,
- (f) Individual Class members may not have the ability or incentive to pursue individual legal action on their own.

PARTICULAR ISSUES – FED. R. CIV. P. 23(C)(4)

147. In the event unforeseen issues preclude class certification under Fed.R.Civ.P. 23(b)(3), the case is still appropriate for class certification under Fed.R.Civ.P. 23(c)(4), as to the particular issues of liability.

148. Defendants have acted or refused to act on grounds generally applicable to Plaintiffs and the other members of the Class, thereby making declaratory relief, as described below, with respect to the Class as a whole.

COUNT I
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT – 18 U.S.C. § 1030
(Defendant Weiss)

149. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

150. Plaintiffs allege that Defendant Weiss violated the Computer Fraud and Abuse Act.

151. Weiss violated the Computer Fraud and Abuse Act by unlawfully accessing Plaintiffs' private information without authorization.

152. Weiss' actions constituted a violation of the Act because by entering the digital network and extracting sensitive private information of students, he "intentionally accesse[d] a computer without authorization" and/or "exceed[ed] authorized access, and thereby obtain[ed] ... information." 18 U.S.C. § 1030(a)(2)(C).

153. Weiss's actions were deliberate because he knew he was unauthorized and proceeded nevertheless.

154. Under 18 U.S.C. § 1030(g), Plaintiffs may recover damages in this civil action from Weiss along with injunctive relief or other equitable relief.

155. Given the willful violations committed by Weiss, resulting in significant damage, harm, humiliation, and distress to Plaintiffs and other Class Members, Plaintiffs should be awarded all appropriate damages in this matter.

COUNT II
VIOLATIONS OF THE STORED COMMUNICATIONS ACT
U.S.C. § 2701 et seq
(Defendants Weiss, University and Keffer)

156. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

157. Plaintiffs allege that Defendants Weiss, University and Keffer violated the Stored Communications Act.

158. The Stored Communications Act, 18 U.S.C. § 2701 et seq., prohibits the unauthorized access of web-based cloud storage and media accounts such as those at issue and other accounts hosted by Defendants University and Keffer that contain personal, private, and intimate information and communications about and relating to Plaintiffs and others situated similarly to Plaintiffs.

159. Specifically, under 18 U.S.C. § 2701(a), it is unlawful for any person to: (1) intentionally access without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceed an authorization to access that facility; and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system.

160. Under 18 U.S.C. § 2702, it is unlawful for a person or entity providing an electronic communication service to the public to knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service or to divulge to any person or entity

the contents of any communication which is carried or maintained on that service on behalf of a subscriber or customer of such service, solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

161. Plaintiffs' electronic information and communications were in electronic storage and clearly fall within the scope of the statute.

162. Defendant Weiss was not authorized to access or divulge the content of Plaintiffs' private communications by for any purpose.

163. The information, messages, files, and media were accessed by Weiss without authorization.

164. Weiss's access without authorization were deliberate.

165. There is no manner in which Plaintiffs' private information, messages, files, and media could have been obtained without unauthorized access and would not have been obtained without unauthorized access had Defendants Keffer and University not knowingly divulged or permitted access to such information, through Keffer Development other channels, despite knowing that the information would not be protected.

166. Under Section 2707 of the Stored Communications Act, individuals may bring a civil action for the violation of this statute.

167. This law imposes strict liability on violators.

168. The statute provides that a person aggrieved by a violation of the act may seek appropriate relief including equitable and declaratory relief, actual damages or damages no less

than \$1,000 punitive damages, and reasonable attorney's fee[s] and other litigation costs reasonably incurred according to 18 U.S.C. § 2707(b)-(c).

169. Defendants' access to and divulging of Plaintiffs' private, personal, and intimate information, messages, files, and media constituted a violation of 18 U.S.C. §§ 2701 and 2702.

170. The University, Keffer and Weiss knew they did not have authority to access and divulge Plaintiffs' private, personal, and intimate information, messages, files, and media but did so anyway.

171. Defendants' knowing or intentional conduct led to multiple violations of the Stored Communications Act.

172. As a result of these violations, Plaintiffs have incurred significant monetary and nonmonetary damages as a result of these violations of the Stored Communications Act, and Plaintiffs seek appropriate compensation for their damages.

173. Under the statute, Plaintiffs should be granted the greater of (1) the sum of their actual damages suffered and any profits made by the University and Weiss as a result of the violations or (2) \$1,000 per violation of the Stored Communications Act.

174. Given these violations were deliberate, the Court should assess punitive damages against Defendants as well.

175. Plaintiffs should also be granted reasonable attorney fees and costs.

**COUNT III – VIOLATION OF TITLE IX, 20 U.S.C. § 1681(A) Et Seq.
(Defendant High Point University)**

176. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

177. Plaintiffs allege that Defendant High Point University and Keffer violated Title IX, 20 U.S.C. § 1681(A) et seq.

178. Defendant High Point University receives federal financial support for its educational programs and is therefore subject to the provisions of Title IX of the Education Act of 1972, 20 U.S.C. § 1681(a), et seq.

179. Title IX mandates that “No person in the United States shall on the basis of sex, be ... subject to discrimination under any education program or activity receiving Federal financial assistance ...”

180. Each Plaintiff and Class Member is a “person” under the Title IX statutory language.

181. Weiss specifically targeted women in his unwanted invasions of privacy and his misconduct is discrimination on the basis of sex.

182. Defendant High Point University, under Title IX, is obligated to investigate allegations of sexual harassment.

183. Defendant High Point University was aware of the sensitive nature of the private and personal information of Plaintiffs to which Weiss was able to access.

184. Defendant High Point University acted with deliberate indifference to sexual harassment by:

- a. Failing to protect Plaintiffs and others as required by Title IX;
- b. Neglecting to adequately investigate and address the complaints regarding the deeply sensitive information Plaintiffs provided;
- c. Failing to institute corrective measures to prevent Weiss from sexually harassing students; and

d. Failing to adequately investigate the other multiple acts of deliberate indifference.

185. Defendant High Point University acted with deliberate indifference as their lack of response to the sexual harassment was clearly unreasonable in light of the known circumstances.

186. Defendant High Point University's failure to promptly and appropriately protect, investigate, and remedy and respond to the sexual harassment of women has effectively denied them equal educational opportunities at the University, including access to medical care and sports training.

187. At the time the Plaintiffs received some medical and/or athletic training services from the University, they did not know the Defendant failed to adequately consider their safety.

188. As a result of Defendant High Point University's deliberate indifference, Plaintiffs have suffered loss of educational opportunities and/or benefits.

189. Plaintiffs have incurred, and will continue to incur, attorney's fees and costs of litigation.

190. At the time of Defendants' misconduct and wrongful actions and inactions, Plaintiffs were unaware, and or with reasonable diligence could not have been aware, of Defendants' institutional failings with respect to their responsibilities under Title IX.

191. Defendant High Point University maintained a policy and/or practice of deliberate indifference to protection of female student athletes.

192. Defendant's policy and/or practice of deliberate indifference to protection against the invasion of privacy for female athletes created a increased risk of sexual harassment.

193. Despite being able to prevent these privacy violations and acts of harassment, Defendant failed to do so.

194. Because of the Defendant High Point University's policy and/or practice of deliberate indifference, Plaintiffs had their privacy invaded and were sexually harassed by Weiss.

195. Plaintiffs should be awarded all such forms of damages in this case for Defendant High Point University's conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

**COUNT IV - VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.
§ 1983 - UNREASONABLE SEARCH AND SEIZURE
(Defendant Weiss)**

196. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

197. Plaintiffs allege Defendant Weiss violated their civil rights under 42 U.S.C. § 1983 and the Fourth Amendment of the U.S. Constitution.

198. Defendant Weiss, sued in his individual capacity, was a state employee at all times relevant to this action, and acted under color of state law to deprive Plaintiffs of their "rights, privileges or immunities secured by the Constitution and laws" of the United States, 42 U.S.C. § 1983, specifically their Fourth Amendment right to be free warrantless and unreasonable searches and seizures.

199. At the time of his actions giving rise to this case, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally searched and seized Plaintiffs' private information without their consent, without a warrant, without probable cause or reasonable suspicion, and without any lawful basis or justification, in violation of Plaintiffs' clearly established rights under the Fourth Amendment.

200. The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated "

201. It is well settled that the Fourth Amendment's protection extends beyond the sphere of criminal investigations. *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 755 (2010) (citing *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 530 (1967)).

202. "The [Fourth] Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government," without regard to whether the government actor is investigating crime or performing another function." *Id.* (quoting *Skinner v. Railway Labor Executives' Assn.*, 489 U.S. 602, 613-614 (1989)).

203. Plaintiffs had a reasonable and legitimate expectation of privacy in their private, personal, and intimate information and images.

204. Acting under color of law, Defendant Weiss violated Plaintiffs' clearly established right not to have their private, personal, and intimate information and images. accessed, searched, viewed, and seized when he searched and seized Plaintiffs' private, personal, and intimate information and images without a warrant, without reasonable suspicion, without probable cause, and without any lawful basis, justification or need to support such an intrusion on Plaintiffs' reasonable and legitimate expectation of privacy in that information.

205. Defendant Weiss's search and seizure of Plaintiffs' personal information was per se unreasonable under the Fourth Amendment.

206. Defendant Weiss' search and seizure of Plaintiffs' private, personal, and intimate information and images was unjustified at its inception and was not related in scope to any circumstances that would justify the search and seizure in the first place.

207. Defendant Weiss is not entitled to qualified immunity because Plaintiffs' rights under the Fourth Amendment not to have their personal information searched and seized by him without a warrant, without permission, and without any lawful basis or justification, was obvious and clearly established when Weiss accessed Plaintiffs' private information, such that no reasonable person in Weiss's position would believe that the act of searching and seizing Plaintiffs' private information was lawful under the specific circumstances presented, and Weiss had fair warning under the law as it existed at the time of his actions that those actions obviously violated Plaintiffs' rights under the Fourth Amendment.

208. As a direct and proximate result of Weiss's violation of Plaintiffs' Fourth Amendment rights, Plaintiffs have suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

209. Plaintiffs should be awarded all such forms of damages in this case for Weiss's conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

**COUNT V -- VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.
§ 1983 - DUE PROCESS/BODILY INTEGRITY
(Defendant Weiss)**

210. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

211. Plaintiffs are alleging Defendant Weiss violated their civil rights under 42 U.S.C. § 1983 and the Fourteenth Amendment of the U.S. Constitution.

212. Defendant Weiss, sued in his individual capacity, was a state employee at all times relevant to this action, and acted under color of state law to deprive Plaintiffs of their "rights, privileges or immunities secured by the Constitution and laws" of the United States, 42 U.S.C. § 1983, specifically their Fourteenth Amendment equal protection right to be free from sexual

harassment in an educational setting, and their Fourteenth Amendment due process right to be free from violation of bodily integrity. *West v. Atkins*, 487 U.S. 42, 49-50 (1988) (quoting *Lugar v. Edmondson Oil Co.*, 457 U.S. 922, 936 n. 18 (1982)).

213. At the time of the actions giving rise to this case, it was obvious, clearly established, and known to Weiss that the right to be free from sexual abuse at the hands of a state employee was protected by the Due Process Clause of the Fourteenth Amendment, such that he knew his actions in accessing Plaintiffs' private, personal, and intimate information and images violated Plaintiffs' fundamental right of due process.

214. At the time of his actions giving rise to this case, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally engaged in actions which violated Plaintiffs' right of bodily integrity, in violation of the Due Process Clause.

215. Weiss's actions were malicious, intentionally harmful, and were taken with deliberate indifference, and were so outrageous as to shock the contemporary conscience.

216. As a direct and proximate result of Weiss's violation of Plaintiffs' Fourteenth Amendment rights, Plaintiffs have suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

217. Plaintiffs should be awarded all such forms of damages in this case for Weiss's conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

**COUNT VI -- VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.
§ 1983 - EQUAL PROTECTION
(Defendant Weiss)**

218. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

219. Plaintiffs are alleging Defendant Weiss violated their civil rights under 42 U.S.C. § 1983 and the Fourteenth Amendment of the U.S. Constitution.

220. Weiss's deliberate and intentional actions in accessing Plaintiffs' personal, private, and intimate images and information constituted sexual harassment and abuse because Weiss accessed Plaintiffs' highly sensitive, private, and personal information, data, and media for his own personal and sexual purposes.

221. At the time of the actions giving rise to this case, it was obvious, clearly established, and known to Weiss that the right to be free from gender discrimination, including sexual harassment and abuse at the hands of a state employee, was protected by the Equal Protection Clause of the Fourteenth Amendment, such that Weiss knew his actions in accessing Plaintiffs' personal, private, and intimate images and information violated Plaintiffs' rights under the Fourteenth Amendment.

222. At the time of his actions giving rise to this case, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally engaged in sexual harassment and sexual abuse, in violation of the Equal Protection Clause.

223. As a direct and proximate result of Weiss's violation of Plaintiffs' Fourteenth Amendment rights, Plaintiffs have suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

224. Plaintiffs should be awarded all such forms of damages in this case for Weiss's conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

**COUNT VII -- VIOLATION OF CIVIL RIGHTS UNDER 42 U.S.C.
§ 1983 - DUE PROCESS/DEPRIVATION OF PROPERTY
(Defendant Weiss)**

225. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

226. Plaintiffs allege that Defendant Weiss violated their civil rights under 42 U.S.C. § 1983 and the Fourteenth Amendment of the U.S. Constitution.

227. Defendant Weiss, sued in his individual capacity, was a state employee at all times relevant to this action, and acted under color of state law to deprive Plaintiffs of their "rights, privileges or immunities secured by the Constitution and laws" of the United States, 42 U.S.C. § 1983, specifically their Fourteenth Amendment due process right to be free of deprivations of property without due process

228. At the time of the actions giving rise to this case, it was obvious, clearly established, and known to Weiss that the right not to be deprived of one's property without due process was protected by the Due Process Clause of the Fourteenth Amendment, such that he knew his actions in accessing and misappropriating Plaintiffs' private, personal, and intimate information and images violated Plaintiffs' fundamental right of due process.

229. Plaintiffs and others similarly situated had a protected property interest in their personal, private, intimate, and confidential information.

230. At the time of his actions giving rise to this case, Weiss was a state actor, functioning in his capacity as a coach and employee of the University of Michigan, when he intentionally engaged in actions which violated Plaintiffs' right not to be deprived of their personal property, in violation of the Due Process Clause.

231. Weiss' actions were malicious, intentionally harmful, and were taken with deliberate indifference, and were so outrageous as to shock the contemporary conscience.

232. As a direct and proximate result of Weiss' violation of Plaintiffs' Fourteenth Amendment rights, Plaintiffs have suffered, and will continue to suffer into the future, damage, humiliation, and embarrassment.

233. Plaintiffs should be awarded all such forms of damages in this case for Weiss' conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

RELIEF

WHEREFORE, Plaintiffs pray this Court grant the following relief:

- a. Enter a judgment encompassing the relief requested above, plus significant compensatory damages exceeding \$5,000,000.00 together with costs, interest and attorney fees, against Defendants, and such other relief to which they are entitled;
- b. An order certifying the proposed Class and Subclasses; designating Plaintiffs as the named representative of the respective Class Members; and appointing her counsel as Class Counsel;
- c. All such equitable relief as the Court deems proper and just, including but not limited to, declaratory relief;
- d. Award Plaintiffs costs, attorney fees as well as interest from the date of Judgment until paid; and
- e. Grant such further relief as is agreeable to equity and good conscience.

JURY DEMAND

For all triable issues, a jury is hereby demanded.

Respectfully Submitted,

BURNS DAY & PRESNELL, P.A.

/s/ James J. Mills
NC BAR NO. 36529
PO Box 10867
Raleigh, NC 27605
919.782.1441 (phone)
919.782.2311 (fax)
Jmills@bdppa.com

SOMMERS SCHWARTZ, P.C.

By: /s/ Lisa M. Esser
Lisa M. Esser (P70628)
Jason J. Thompson (P47184)
Attorneys for Plaintiffs
One Towne Square, 17th Floor
Southfield, MI 48076
(248) 355-0300
LEsser@sommerspc.com
JThompson@sommerspc.com

Pro Hac Vice application pending

Megan Bonanni (P52079)
Kevin M. Carlson (P67704)
Attorneys for Plaintiffs
117 W. Fourth Street, Suite 200
Royal Oak, MI 48067
(248) 398-9800
mbonnani@pittlawpc.com
kcarlson@pittlawpc.com

Pro Hac Vice application pending

Dated: April 23, 2025

From: U.S. Department of Justice - VNS fedemail@vns.usdoj.gov
Subject: [EXTERNAL] U.S. Department of Justice - VNS - Investigative Case
288A-DE-3728795
Date: Nov 10, 2024 at 2:59:42 PM

This email is from an external source. Only open links and attachments from a Trusted Sender.
DO NOT REPLY TO THIS EMAIL.



November 10, 2024

U.S. Department of Justice
Federal Bureau of Investigation
Detroit Division
477 Michigan Ave
26th Floor
Detroit, MI 48226
Phone: DE-CYVictim@fbi.gov
Email: DE-CYVictim@fbi.gov

RE: Case Number: 288A-DE-3728795

Dear _____ :

As a Victim Specialist with the Federal Bureau of Investigation (FBI), Victim Services Division (VSD), Detroit Division, I am contacting you because you have been identified as a possible victim of a federal crime. The FBI is responsible for ensuring that victims receive information and services during the investigation of a federal crime while being treated with dignity and respect.

As a possible victim of a federal crime, you are legally entitled to receive certain services and assistance including notifications on the case listed above. We will make every effort to keep you informed about the case to the extent that we can while not interfering with the investigation. We are also committed to providing you with support and information about available services, programs, and resources. Please contact me if you would like information or referrals for services in your area.

Throughout the investigation you may receive multiple notifications. The purpose of this initial letter is to notify you that this case is currently under investigation. If the investigation results in the filing of federal charges, notifications will be sent to you by the United States Attorney's Office.

If you have questions about this notification or would like information about available resources, you can contact DE-CYVictim@fbi.gov. If you would like to verify the legitimacy of this notification, please contact the FBI Detroit Field Office at [\(313\) 965-2323](tel:3139652323). You can also find this phone number listed on FBI Detroit's website.

Due to the large number of potential victims in this case, you will likely not receive additional correspondence by mail. Updates will continue to be available in VNS, through your profile or by email. VNS must have an email address on file to send updates and notifications by email. You can verify or enter your email address by logging into VNS and updating your contact information.

Below you will find information on the Victim Notification System (VNS). VNS is designed to keep victims informed about their case. The system incorporates outgoing notifications such as this letter, a call center, and an online tool. The call center and online tool also allow you to update your contact information and notification preferences. Through VNS, please remember that you may choose to stop or resume notifications at any time. Given the sensitivity of some information, case status information available through VNS may be very limited. Lastly, if you wish to receive important notifications in your case, it is your individual responsibility to maintain current contact information in the system.

Current information regarding the status of your case can be found on the Internet at <https://www.notify.usdoj.gov> or by calling the Victim Notification System (VNS) Call Center at [1-866-DOJ-4YOU](tel:1866DOJ4YOU) ([1-866-365-4968](tel:18663654968)). You will need to enter your Victim Identification Number (VIN) ' ' and your Personal Identification Number (PIN) ' ' anytime you contact the Call Center and the first time you log into VNS on the Internet. If you are receiving notifications with multiple victim ID/PIN codes please contact the VNS Call Center. In addition, the first time you access the VNS Internet site, you will be prompted to enter your last name (or business name) as currently contained in VNS. The name you should enter is .

You can also use the Call Center and the Internet to correct/update your contact information and/or change your decision regarding participation in the notification system. Your participation in this notification system is totally voluntary. You can choose not to participate or reactivate your access at any time. In order to continue to receive notifications, it is your responsibility to keep your contact information current.

The email address VNS currently has for you is . If this address is correct and you have not received an email from VNS within four days of the date of this letter, please check your junk/spam folder and accept emails from fedemail@vns.usdoj.gov. If the email address provided above is incorrect, please update the email address by accessing the VNS Web site. This email address has not been verified in VNS and future emails will not contain details about the nature of the notification. To receive subsequent emails with the full text of the notification you must verify this email address by accessing the VNS Internet web page using the login information provided above.

Once you have verified/updated your email address, most, if not all, future notifications will be provided by email and not by letter. If you do not verify your email address, VNS will continue (in most cases) to send letter and email notifications. However, when an email address is not verified, future emails will not contain details about the nature of the notification.

If you have additional questions related to this matter, please contact me at DE-CYVictim@fbi.gov. When you call, please provide the file number located at the top of this letter.

Sincerely,

Nicole McGee
Victim Specialist

If you do not want to receive email notifications from the Victim Notification System (VNS) please log into the VNS Web site at <https://www.notify.usdoj.gov>, select "My Information", remove your email address and click the "update" button. If you remove your email address, you will continue to receive letters from VNS except in those case which have large numbers of victims. To change your email address, select "My Information", provide a new address and click the "update" button.

If you do not want to receive any notifications in your case, select "Stop Receiving Notifications" and follow the instructions on the screen.

If you believe you have received this email in error, please contact the office listed at top of the email message.

Please note, if this is the first notification you have received from VNS you will need to wait 4-8 hours from receipt of this email before you can login to the VNS Internet site (<https://www.notify.usdoj.gov>). In addition, it will also be 4-8 hours before any documents which may have been uploaded to VNS as part of this notification are available under the "Downloads/Links" section on the Web page.

Please call the Victim Notification System (VNS) Help Desk at phone number [1-866-625-1631](tel:1-866-625-1631) for assistance and questions.

Attachments have been referenced with this notification and are available on the VNS Internet site (or will be available within 8 hours). After you log into the website select "Downloads/Links" to view the attachments.

----- Forwarded message -----

From: **U.S. Department of Justice - VNS** <fedemail@vns.usdoj.gov>

Date: Wed, Mar 26, 2025 at 4:27 PM

Subject: U.S. Department of Justice - VNS - Investigative Case 288A-DE-3728795 - Court Case 25-CR-20165

To: [REDACTED]

DO NOT REPLY TO THIS EMAIL.



March 26, 2025

U.S. Department of Justice

Eastern District of Michigan

Suite 2001

211 W. Fort St.

Detroit, MI 48226-3211

Phone: 1-844-527-5299

Email: USAEO.MCAP@usdoj.gov

[REDACTED]

Re: United States v. Defendant(s) Matthew Weiss
Case Number 2023R00208 and Court Docket Number 25-CR-20165

Dear [REDACTED]

The enclosed information is provided by the United States Department of Justice Victim Notification System (VNS). As a victim witness professional, my role is to assist you with information and services during the prosecution of this case. I am contacting you because you were identified by law enforcement as a victim or potential victim during the investigation of the above criminal case.

Should you have questions concerning this case, please contact the Mega Victim Case Assistance Program (MCAP) toll free 1-844-527-5299 (Monday through Friday from 8:30 am to 5:30 pm Eastern), or send an email to USAEO.MCAP@usdoj.gov. Please include your Victim Identification Number (VIN), found in the closing paragraph of this notification, when contacting MCAP via phone or email. If you are having technical difficulties with the Victim Notification System, please contact the VNS Help Desk at the numbers found in the closing of this notification.

Charges have been filed against defendant(s) Matthew Weiss. The lead prosecutor for this case is Timothy Wyse. The main charge is categorized as Other White Collar Crime/Fraud.

If you are receiving this notification, it means that information of yours was found in possession of the defendant.

Pursuant to the Crime Victims' Rights Act, found at Title 18 U.S.C. § 3771, victims have the following rights:

(1) The right to be reasonably protected from the accused; (2) The right to reasonable, accurate, and timely notice of any public court proceeding, or any parole proceeding, involving the crime or of any release or escape of the accused; (3) The right not to be excluded from any such public court proceeding, unless the court, after receiving clear and convincing evidence, determines that testimony by the victim would be materially altered if the victim heard other testimony at that proceeding; (4) The right to be reasonably heard at any public proceeding in the district court involving release, plea, sentencing, or any parole proceeding; (5) The reasonable right to confer with the attorney for the Government in the case; (6) The right to full and timely restitution as provided in law; (7) The right to proceedings free from unreasonable delay; (8) The right to be treated with fairness and with respect for the victim's dignity and privacy; (9) The right to be informed in a timely manner of any plea bargain or deferred prosecution agreement; and (10) The right to be informed of the rights under this section and the services described in section 503(c) of the Victims' Rights and Restitution Act of 1990 (34 U.S.C. § 20141 (c)) and provided contact information for the Office of the Victims' Rights Ombudsman of the Department of Justice.

We will make our best efforts to ensure you are provided the rights to which you are entitled by law. Please understand that these rights apply only to victims of the counts charged in federal court. If you have any questions about what this means for you, please contact our office. Separately, victims of all crimes under federal investigation are entitled to services under the Victims' Rights and Restitution Act (VRRRA), including notification of court events. For further details, please refer to Title 34 U.S.C. § 20141 or the VRRRA link posted at www.notify.usdoj.gov (under the "Related Links" tab, see "Victim Rights").

It is important to keep in mind that the defendant(s) is/are presumed innocent until proven guilty. Additionally, please be aware that many criminal cases are resolved by a plea agreement between the prosecutor's office and the defendant. You should also know that it is not unusual for a defendant to seek to negotiate a plea agreement shortly before a trial is scheduled to begin. If the court schedules a plea hearing in this case, we will make our best efforts to notify you as soon as practicable.

As mentioned above, you have the right to confer with the attorney for the government. If you would like to speak with the prosecutor to inform the prosecutor of your views regarding potential plea agreements or discuss any other aspect of the case, please contact our office at 1-844-527-5299 and ask to speak to the victim assistance staff, and we will arrange for you to speak with the prosecutor. While our office cannot act as your attorney or provide you with legal advice, you can seek the advice of an attorney with respect to the rights described above or other related legal matters.

If you believe that a Department of Justice employee has not provided you with your rights under the Crime Victims' Rights Act, you may file a complaint with the Department of Justice Victims' Rights Ombudsman (or "Ombuds"). For more information, go to www.justice.gov/usao/office-victims-rights-ombuds. If you have questions about filing a complaint, you may contact the Ombudsman by phone at 1-

877-574-9302 or by email at USAEO.VictimOmbudsman@usdoj.gov.

If you have questions about the progress of your case, the rights you are entitled to, or how you can assert your rights during court proceedings, please contact our office at 1-844-527-5299.

Custody of a defendant during a federal criminal case is determined by the Court and is managed by the United States Marshal Service. Custody status of a defendant is subject to change during the course of the criminal proceedings. To receive the timeliest update to your case, please provide and verify your email address, as instructed below.

As of March 24, 2025, Matthew Weiss is not in the custody of the U.S. Marshal Service.

Due to the large number of victims this office receives, you will likely not receive additional correspondence by mail but notice will continue to be available by the other means provided by VNS including email. Through the Victim Notification System (VNS) we will continue to provide you with updated scheduling and event information as the case proceeds through the criminal justice system. You may obtain current information about this case on the VNS website at <https://www.notify.usdoj.gov> or from the VNS Call Center at 1-866-DOJ-4YOU (1-866-365-4968) (TDD/TTY: 1-866-228-4619) (International: 1-502-213-2767). In addition, you may use the Call Center or Internet to update your contact information and/or change your decision about participation in the notification program.

You will use your Victim Identification Number (VIN) [REDACTED] and Personal Identification Number (PIN) [REDACTED] anytime you contact the Call Center and the first time you log into VNS on the website. If you are receiving notifications with multiple victim ID/PIN codes please contact the VNS Call Center. In addition, the first time you access the VNS website, you will be prompted to enter your last name (or business name) as currently contained in VNS. The name you should enter is Kane.

Remember, VNS is an automated system and cannot answer questions. If you have other questions which involve this matter, please contact this office at the number listed above.

Sincerely,

Alexandra Wyatt
Victim Services Coordinator

If you do not want to receive email notifications from the Victim Notification System (VNS) please log into the VNS Web site at <https://www.notify.usdoj.gov>, select "My Information", remove your email address and click the "update" button. If you remove your email address, you will continue to receive letters from VNS except in those case which have large numbers of victims. To change your email address, select "My Information", provide a new address and click the "update" button.

If you do not want to receive any notifications in your case, select "Stop Receiving Notifications" and follow the instructions on the screen.

If you believe you have received this email in error, please contact the office listed at top of the email message.

Please note, if this is the first notification you have received from VNS you will need to wait 4-8 hours from receipt of this email before you can login to the VNS Internet site (<https://www.notify.usdoj.gov>). In addition, it will also be 4-8 hours before any documents which may have been uploaded to VNS as part of this notification are available under the "Downloads/Links" section on the Web page.

Please call the Victim Notification System (VNS) Help Desk at phone number 1-866-625-1631 for assistance and questions.

Attachments have been referenced with this notification and are available on the VNS Internet site (or will be available within 8 hours). After you log into the website select "Downloads/Links" to view the attachments.

[Query](#) [Reports](#) [Utilities](#) [Help](#) [Log Out](#)

**United States District Court
District of Massachusetts (Boston)
CIVIL DOCKET FOR CASE #: 1:25-cv-11151-JEK**

Doe v. Weiss et al
Assigned to: District Judge Julia E. Kobick
Demand: \$5,000,000
Cause: 18:1030 Violation of Computer Fraud and Abuse Act

Date Filed: 04/28/2025
Jury Demand: Plaintiff
Nature of Suit: 890 Other Statutory Actions
Jurisdiction: Federal Question

Plaintiff

Jane Doe

*individually and on behalf of all others
similarly situated*

represented by **Paula S. Bliss**

Justice Law Collaborative, LLC
210 Washington Street
North Easton, MA 02356
508-230-2700
Email: paula@justicelc.com
ATTORNEY TO BE NOTICED

V.

Defendant

Matthew Weiss

Defendant

Simmons University

Defendant

The Trustees of Simmons University

Defendant

Keffer Development Services, LLC

Date Filed	#	Docket Text
04/28/2025	1	COMPLAINT against Matthew Weiss, Keffer Development Services, LLC, The Trustees of Simmons University, Simmons University Filing fee: \$ 405, receipt number AMADC-10976172 (Fee Status: Filing Fee paid), filed by Jane Doe. (Attachments: # 1 Civil Cover Sheet, # 2 Category Form, # 3 DOJ Data Breach Notice, # 4 Keffer's Athletic Trainer System Brochure, # 5 Keffer's Company History, # 6 Keffer's Website Home Page, # 7 Keffer's FAQ Page, # 8 Keffer's Privacy Policy)(Bliss, Paula) (Entered: 04/28/2025)
04/28/2025	2	MOTION to Proceed Under Pseudonym re 1 Complaint,, by Jane Doe.(Bliss, Paula) (Entered: 04/28/2025)
04/28/2025	3	MEMORANDUM in Support re 2 MOTION to Proceed Under Pseudonym re 1 Complaint,, filed by Jane Doe. (Bliss, Paula) (Entered: 04/28/2025)

04/28/2025	4	ELECTRONIC NOTICE of Case Assignment. District Judge Julia E. Kobick assigned to case. If the trial Judge issues an Order of Reference of any matter in this case to a Magistrate Judge, the matter will be transmitted to Magistrate Judge Donald L. Cabell. (SEC) (Entered: 04/28/2025)
04/28/2025	5	Summons Issued as to Keffer Development Services, LLC, Simmons University, The Trustees of Simmons University, Matthew Weiss. Counsel receiving this notice electronically should download this summons, complete one for each defendant and serve it in accordance with Fed.R.Civ.P. 4 and LR 4.1. Summons will be mailed to plaintiff(s) not receiving notice electronically for completion of service. (SP) (Entered: 04/28/2025)
05/02/2025	6	MOTION to Appoint Counsel by Jane Doe.(Bliss, Paula) (Entered: 05/02/2025)
05/02/2025	7	MEMORANDUM in Support re 6 MOTION to Appoint Counsel filed by Jane Doe. (Attachments: # 1 Weiss Indictment, # 2 Jane Doe 1, et al, v. Matthew Weiss, et al., 1:25-cv-04233 (N.D. Ill.), # 3 Jane Doe 1, et al., v. Matthew Weiss, et al., Case No. 5:25-cv-00997 (C.D. CA), # 4 Jane Doe, et al. v. Matthew Weiss, et al., Case No. 1:25-cv-11151 (D. MD), # 5 Janes Does 1 and 2, et al. v. Matthew Weiss, et al., No. 25-cv-303 (MDNC), # 6 Case Management Conference Order, # 7 Tentative Joint Submission, # 8 Motion for Case Management Conference, # 9 Sommers Schwartz Bio, # 10 Pitt McGehee Palmer Bonanni & Rivers Bio, # 11 Justice Law Collaborative Dougherty Bio, # 12 Proposed Order)(Bliss, Paula) (Entered: 05/02/2025)
05/27/2025	8	WAIVER OF SERVICE Returned Executed by Jane Doe. Keffer Development Services, LLC waiver sent on 5/23/2025, answer due 7/22/2025. (Dougherty, Kimberly) (Entered: 05/27/2025)

PACER Service Center			
Transaction Receipt			
06/05/2025 16:23:31			
PACER Login:	ThomaKingking	Client Code:	
Description:	Docket Report	Search Criteria:	1:25-cv-11151-JEK
Billable Pages:	2	Cost:	0.20

**UNITED STATES DISTRICT COURT
DISTRICT COURT OF MASSACHUSETTS**

JANE DOE,
*individually and on
behalf of all others similarly situated,*

Plaintiff,

v.

MATTHEW WEISS; the TRUSTEES OF
SIMMONS UNIVERSITY; SIMMONS
UNIVERSITY; and KEFFER
DEVELOPMENT SERVICES, LLC,

Defendants.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Civil Action No.

Plaintiff Jane Doe¹ brings this lawsuit on behalf of herself and all others who have been subjected to an unlawful breach of privacy, stemming from former University of Michigan and Baltimore Ravens coach Matthew Weiss' unauthorized access of athletic trainer databases maintained by a third-party vendor, Keffer Development Services, LLC. Plaintiff files this class action complaint and alleges the following.

NATURE OF THE ACTION

Students and alumni connected to Simmons University from 2015 to 2023—many of them student-athletes—have been subjected to a deeply troubling and unlawful breach of privacy, stemming from the actions of former University of Michigan and Baltimore Ravens coach Matthew Weiss, whose gross and despicable violations of their privacy were facilitated by institutional negligence. This class action lawsuit, filed against Matthew Weiss, Simmons

¹ Jane Doe is a pseudonym. Plaintiff's motion seeking leave to proceed pseudonymously is forthcoming.

University and its Trustees, and Keffer Development Services, LLC, seeks justice for the unauthorized access and misuse of personal information—an abuse so severe that students and student-athletes across the nation are now receiving formal notification from the U.S. Department of Justice that their private information, including intimate photos and videos, have been exposed, including Plaintiff Jane Doe. This action is brought to hold the Defendants accountable for failing to protect their students from foreseeable harm.

PARTIES

1. Plaintiff Jane Doe was a student athlete at Simmons University between 2012 and 2016 and was a member of the Cross Country Team.

2. Plaintiff Jane Doe is domiciled in Plymouth County, Massachusetts.

3. Defendant Simmons University (“Simmons”) is a school incorporated in Massachusetts with its principal place of business located at 300 The Fenway, Boston, Massachusetts. Simmons University was Simmons College and renamed Simmons University in or around 2017.

4. Defendant Trustees of Simmons University are sued in their official capacity as Trustees of Simmons University.

5. Defendant Keffer Development Services, LLC (“Keffer”) is a Pennsylvania limited liability company with its principal place of business in Grove City, PA, that has continuously and systemically conducted business in Massachusetts by directly providing services to residents and entities within the Commonwealth of Massachusetts, thereby availing itself of protections of the law of the Commonwealth of Massachusetts. Defendant Keffer is a technology and data vendor operating an electronic medical record and student athlete training system, which stored the personally identifiable information (“PII”) and protected health information (“PHI”) of Plaintiff

and Class Members across the country. Any wrongful conduct and legal violations committed by Defendant Keffer that are subsequently outlined in this Complaint occurred specifically with respect to the Plaintiff during the time of the incident alleged in this Complaint.

6. Matthew Weiss (“Weiss”) is an individual domiciled in the State of Michigan, who had affirmative contacts with the Commonwealth of Massachusetts in that he conducted illegally activity in the Commonwealth of Massachusetts, by hacking into the personal property of Plaintiff and putative Class Members of the Commonwealth of Massachusetts during the applicable time period at issue in this Complaint and said activities of which this Complaint arises from.

7. On March 20, 2025, Defendant Weiss was indicted on 24 counts of unauthorized access to computers and aggravated identity theft by the U.S. Attorney for the Eastern District of Michigan.

JURISDICTION AND VENUE

8. Jurisdiction is proper in this Court under 28 U.S.C. §§ 1331 and 1367 as this matter involves a claim under the Stored Communications Act, 18 U.S.C. § 2701(a) *et seq.*; the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; Title IX, 20 U.S.C. § 1681(A) *et seq.*; and this Court has supplemental jurisdiction of all additional causes of action alleged in this Complaint pursuant to 28 U.S.C. §1367(a).

9. This Court also has subject matter jurisdiction pursuant to 28 U.S.C. §1332(d) under the Class Action Fairness Act (“CAFA”) as a class action lawsuit in which the amount in controversy exceeds \$5,000,000.00, there are more than one-hundred putative Class Members, and the majority of the putative Class Members are citizens of a state different than the state of which Defendants are citizens.

10. The Court has personal jurisdiction over Defendants named in this action because Defendant Simmons is located and created under the laws of the Commonwealth of Massachusetts, Defendant Weiss had minimum contacts with the Commonwealth of Massachusetts as set forth above, thus purposefully availing himself of the privilege of conducting activities in the Commonwealth of Massachusetts. Defendant Keffer directs business at the Commonwealth of Massachusetts, conducts substantial business in Massachusetts, and has availed itself of the protections of Massachusetts state law. The conduct by Defendant Keffer which gives rise to the claims against Defendant Keffer in this Complaint was directed at and occurred in the Commonwealth of Massachusetts.

11. Venue is appropriate in this District Court under 28 U.S.C. §1391(b) since Defendant Simmons University resides within this District and a substantial part of the events or omissions giving rise to these claims occurred within this District.

12. Plaintiff's injuries are redressable by monetary compensation, and all alleged injuries of Plaintiff and Class Members can be traced to Defendants' conduct.

COMMON ALLEGATIONS

A. Weiss's Data Breach and Cyber Voyeurism of Thousands of Students were Enabled by Defendant Keffer's Failures

13. Plaintiff brings this class action against Defendants Simmons and Keffer for their failure to properly secure the highly sensitive personally identifiable information ("PII") and protected health information ("PHI") of more than 150,000 students, including herself, which Matthew Weiss, former University of Michigan and Baltimore Ravens coach and sexual predator, targeted, unauthorizedly accessed, and stole over the course of nearly a decade.

14. Between 2015 and January 2023, Defendant Weiss gained unauthorized access to databases used by athletic trainers at more than 100 colleges and universities, some of which were maintained by Defendant Keffer, a third-party vendor contracted by these colleges and universities.

15. Upon information and belief, Defendant Simmons contracted with Defendant Keffer.

16. After gaining access to these databases, Weiss downloaded the PII and PHI of more than 150,000 athletes.

17. Using the information that Weiss obtained from the Athletic Trainer System, Weiss was able to target more than 2,000 student athletes and hack their social media, email, and/or cloud storage accounts. Defendant Weiss also illegally obtained access to the social media, email, and/or cloud storage accounts of more than 1,300 additional students and/or alumni from universities and colleges across the country.

18. Defendant Weiss primarily targeted female college athletes. He researched and targeted these women based on their school affiliation, athletic history, physical characteristics, and sexual preferences.

19. Through this scheme, and unknown to students and student athletes, Defendant Weiss downloaded personal, intimate digital photographs and videos that were never intended to be shared beyond intimate partners. This scheme appears to be the largest incident of cyber voyeurism of student athletes in U.S. history.

20. The data breach and cyber voyeurism of over 150,000 students from university and college databases, including athletic databases maintained by Keffer, and the targeted stealing of intimate, personal, digital photographs and videos of 3,300 students and athletes, continued for

26. Defendant Keffer was founded in 1994 and has collaborated with over 600 clients across 48 states and internationally since that time.⁴ Defendant Keffer advertises that it currently serves over 6,500 schools, clinics, and other organizations with over 27,000 users and 2 million athletes.⁵

27. Upon information and belief, the universities served by Keffer include Defendant Simmons, Jane Doe’s alma mater.

28. Keffer represents that its Athletic Trainer System tool was “[d]esigned with Athletic Trainers for ALL Medical Professionals,” and is designed to store PII and PHI belonging to students including their treatment histories, diagnoses, injuries, photos, insurance information, immunizations, and personal details, like height and weight, mental health information, and demographic information.⁶

29. In Keffer’s FAQ, it boasts that “[i]nformation security is a high priority in our company.”⁷ Keffer further claims that “[o]n top of our Data Center being FedRamp Certified, ATS is also HIPAA and FERPA compliant. We utilize a company called Compliance Helper to ensure we maintain HIPAA and FERPA compliance.”⁸

30. In Keffer’s Privacy Policy, it acknowledges that it has obligations as a “business associate” under HIPAA: “To the extent that [Keffer] receives or maintains patient medical information in the course of providing the Clinical EMR, that information is secured, used and

⁴ Keffer’s Company History page on its website is attached as **Exhibit C**.

⁵ Keffer’s home page on its website is attached as **Exhibit D**.

⁶ *Id.*

⁷ Keffer’s FAQ page on its website is attached as **Exhibit E**.

⁸ *Id.*

disclosed only in accordance with [Keffer's] legal obligations as a 'business associate' under HIPAA."⁹

31. Keffer's Privacy Policy further states: "[Keffer] understands that storing our data in a secure manner is essential. KDS stores PII, PHI and other data using industry-standard physical, technical and administrative safeguards to secure data against foreseeable risks, such as unauthorized use, access, disclosure, destruction or modification."¹⁰

32. Despite touting these obligations, Keffer failed to implement basic industry standards to protect student's—including Jane Doe's—PII and PHI.

33. As an example, while Keffer maintained the option to incorporate two-factor authentication to access its Athletic Trainer System applications, it did not require that institutions and users do so.¹¹

34. Two-factor authentication is a basic security measure that requires an additional piece of evidence, known as a factor, such as a code sent via text message or email, before allowing access to the authenticated system.¹²

35. Critically, requiring this security feature could have prevented Defendant Weiss from gaining access to student protected health information with only the access credentials belonging to other administrators and users.

36. Defendants knew that Keffer did not require institutions and users to use two-factor authentication to access the private information and communications accessible through its system, including information maintained in Defendant Simmons's facilities, and thus knowingly and

⁹ Keffer's Privacy Policy is attached as **Exhibit F**.

¹⁰ *Id.*

¹¹ See **Exhibit E**.

¹² Microsoft, *The Importance of Two-Factor Authentication*, July 8, 2022, <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/importance-of-two-factor-authentication>.

deliberately permitted Plaintiff's confidential information and communications to be accessed, shared, and divulged without authorization from Plaintiff.

37. Recent actions by the Federal Trade Commission ("FTC") underscore the gross negligence and failings of Keffer and Defendant Simmons in failing to ensure that the Athletic Trainer System was configured to default to two-factor or multi-factor authentication for access to its systems containing PII and PHI. In February 2023, the FTC published an article highlighting the importance of multi-factor authentication ("MFA") and stating: "[m]ulti-factor authentication is widely regarded as a critical security practice because it means a compromised password alone is ***not enough*** to take over someone's account."¹³

38. Additionally, the FTC's enforcement actions over the past five years further emphasize the critical and fundamental role MFA plays in an effective data security system, where the FTC has ordered MFA be implemented as part of settlements announced in its data security enforcement actions.¹⁴

39. Keffer also lacked any effective data auditing controls to monitor activity on its systems, which would have allowed it to detect the massive, years-long data breach on its systems by Defendant Weiss and the resulting cyber voyeurism on Plaintiff Jane Doe and those Class Members similarly situated.

40. Both Keffer and Defendant Simmons had a responsibility and duty to protect the private data of student athletes stored within their systems and to have controls in place to prevent gross invasions of privacy as occurred in this case.

¹³Alex Gaynor, *Security Principles: Addressing Underlying Causes of Risk in Complex Systems*, FEDERAL TRADE COMMISSION, Feb. 1, 2023, <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems> (emphasis added).

¹⁴Jim Dempsey, *The FTC's rapidly evolving standards for MFA*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, Nov. 8, 2022, <https://iapp.org/news/a/the-ftcs-rapidly-evolving-standards-for-mfa/>.

41. The risk of identity theft and security breaches to access users' private, personal, and confidential information is foreseeable within Simmons and Keffer's information technology systems, and Simmons and Keffer are well aware of the foreseeable risks of data breaches, such as those alleged in this case, that are likely to occur if their practices in detecting, preventing, and mitigating such data breaches are substandard.

C. Defendant Simmons's Failed to Safeguard its Students' Private Information for Nearly a Decade

42. Simmons is a high-level educational institution, with a diverse athletic program, enrolling hundreds of student athletes at any one time across over a dozen sports.

43. In maintaining its highly regarded athletics department and programs, Simmons provides its student athletes with athletic trainers.

44. Simmons had a responsibility and duty to oversee its operations, policies, and procedures, and care for and protect its students.

45. Simmons was required to ensure that students, such as Jane Doe, were not exposed to sexual predators who would invade their privacy.

46. Simmons failed in this duty by failing to take any reasonable action to prevent the harm caused to Jane Doe and other Class Members as alleged in this Complaint.

47. This prolific and egregious breach and violation was entirely preventable by Simmons and Keffer. As noted in a criminal complaint filed by the U.S. Attorney for the Eastern District of Michigan, Defendant Weiss breached the authentication systems of Keffer's and of colleges and universities across this nation by exploiting passwords and other vulnerabilities in their authentication processes. On information and belief, neither Simmons nor Keffer required

that its employees or students implement safeguards like multi-factor authentication to access accounts, a standard practice for all entities collecting PII, especially medical data and PHI.

48. The breach and cyber voyeurism were a direct result of Simmons's and Keffer's failure to implement adequate and reasonable security procedures and protocols necessary to protect Jane Doe and Class Members PII and PHI, leaving the most sensitive and personal information of students, like Jane Doe, vulnerable to exploitation by malicious predators like Defendant Weiss.

49. Simmons was grossly negligent on two fronts: (1) in its hiring and oversight of Keffer, and its entrustment of students' PII and PHI to Keffer; and (2) in its maintenance, oversight, and security of its own internal systems to protect student PII and PHI.

50. Simmons took no reasonable actions to prevent this unauthorized access beforehand despite its duties to students and since discovery of the breaches, has taken no reasonable actions to notify or rectify harm to the victims of Weiss's misconduct and predation.

51. Thousands of students still remain at risk because Simmons and Keffer have failed to undertake any reasonable review of how Jane Doe's private and personal information is secured and who can access such information, and from where.

52. Upon information and belief, to this day, Simmons has not formally informed Class Members impacted by Weiss's cyber voyeurism and misconduct.

D. Simmons was Negligent in Hiring/Contracting with Defendant Keffer and in Entrusting Students PII and PHI to Keffer

53. Simmons provided its student athletes medical treatment, including from athletic trainers.

54. To facilitate that treatment, Simmons contracted with Keffer to use its Athletic Training System application, which required that student athletes provide Simmons and Keffer with sensitive PII and PHI.

55. When collecting that information, Simmons, like Keffer, accepted an obligation to protect that information under contract and statutory principles, including as a “business associate” under HIPAA.

56. Jane Doe and others similar to her entrusted that Simmons and Keffer would safeguard her private information and ensure the security and confidentiality of her data.

57. Simmons and Keffer had, and continue to have, a duty to protect Jane Doe and to take appropriate security measures to protect private, personal, medical and intimate information, communications, and images.

58. Simmons knowingly and deliberately permitted access to and the divulging of Plaintiffs’ stored communications through Keffer and failed to take reasonable action to ensure that Keffer protected the privacy of the sensitive information of Jane Doe and others like her.

59. Upon information and belief, Simmons failed to properly investigate Keffer, Keffer’s protocols, and failed to adequately monitor or establish safeguards for Keffer’s work with the students and their private information to ensure they carried out their duties to safeguard and protect the private information of their students entrusted to them.

60. Simmons was negligent and/or reckless in failing to ensure that media and other private, personal and sensitive information, including but not limited to those of Jane Doe, was securely protected, as Simmons was entrusted to do.

61. Simmons failed to implement security measures necessary to protect their students PII and PHI, including failing to train staff and employees on securing credentials, requiring multi-

or two-factor authentication to use Keffer's Athletic Trainer System, overseeing third-party vendors like Keffer, in which Simmons entrusted students sensitive PII and PHI, and monitoring and auditing access to student files and other private information.

62. In other words, Simmons not only failed to ensure it had implemented sufficient security protocols and procedures across its own systems and staff, but also Simmons failed to ensure Keffer had adequate security measures in place to protect Simmons students' PII and PHI from theft and misuse.

63. Indeed, Simmons lacked adequate training programs to detect and stop breaches like those caused by Defendant Weiss.

64. Simmons and Keffer failed to implement reasonable protective measures to detect Weiss' irregular activity and trespassing, including but not limited to, appropriate authentication tools, behavioral analytics, anomaly detection, machine learning, and real-time monitoring of user activity, looking for deviations from established patterns and suspicious actions, like unusual or repeated login attempts or access to sensitive data, any of which could have prevented Weiss' improper access to private student information.

65. Because both Keffer and Simmons failed to implement basic, industry standard security measures, these Defendants allowed an alleged sexual predator, ex-football coach Matthew Weiss, to access students', particularly female student athletes', most sensitive information for nearly a decade.

66. All Defendants disregarded the rights of Jane Doe and Class Members. Simmons and Keffer knowingly, intentionally, willfully, recklessly and/or negligently provided access to and/or divulged Plaintiffs' private communications stored in their facilities; failed to take adequate and reasonable measures to ensure their data systems were protected against unauthorized

intrusions; failed to disclose that they did not have adequately robust computer systems and security practices to safeguard private information; failed to take standard and reasonably available steps to prevent the data breach and cyber voyeurism; failed to properly train their staff and employees on proper security measures; and failed to provide Jane Doe and the Class Members prompt notice of the data breach and cyber voyeurism.

67. Simmons's and Keffer's conduct amounts to a violation of the duties they owed to Jane Doe under common law tort claims and state and federal statutory law, rendering them liable to Jane Doe and the Class Members for the harms caused by this egregious and preventable cyber voyeurism and invasion of privacy. Defendant Weiss is equally liable for the harms inflicted on Jane Doe and the Class Members by his intentional hacking and theft of their private information under tort and statutory law.

68. Jane Doe and the punitive Class Members are current and former students at Simmons and other affected institutions in the United States that were specifically targeted by Weiss and harmed by the violation of their privacy.

69. Jane Doe and the punitive Class Members suffered injury as a result of Defendants' conduct. These injuries included: invasion and loss of privacy, loss of dignity, humiliation, embarrassment, and severe emotional distress.

70. Jane Doe seeks to remedy these harms on behalf of herself and all similarly situated individuals whose private information was accessed by Weiss.

71. Jane Doe seeks remedies including, but not limited to, compensatory damages, nominal damages, punitive damages, and reimbursement of out-of-pocket costs. Jane Doe 1 also seeks injunctive and equitable relief to prevent future injury on behalf of herself and the putative Class Members.

E. Jane Doe's Allegations

72. Plaintiff Jane Doe is a former student athlete at Simmons.

73. While in school at Simmons, Jane Doe participated in the Cross-Country program while Defendant Weiss's data breach and cyber voyeurism was ongoing.

74. As a student athlete, Jane Doe received treatment from Simmons's athletic trainer staff, requiring her to disclose information about her treatment, including height, weight, injuries, medications, treatment plans, and analysis on performance and recovery. To receive treatment, Jane Doe was required to use the Keffer Athletic Trainer System, and the PII and PHI Jane Doe disclosed was saved on the Keffer Athletic Trainer System.

75. As a student, Jane Doe was required to disclose personal information to Simmons and was issued a Simmons email account where she stored sensitive, personal information.

76. Because Keffer and Simmons never implemented the security safeguards needed to protect Jane Doe's PII and PHI, Defendant Weiss compromised the PII and PHI belonging to every student whose information was saved by Simmons and/or Keffer's Athletic Trainer System, including, on information and belief, Jane Doe's private and personal information.

77. Defendant Weiss compromised all information that was saved in Simmons and/or Athletic Trainer System databases, including Plaintiff's treatment information, injury information, height, weight, and other highly sensitive information.

78. Jane Doe has received notice from the U.S. Department of Justice Victim Notification System that she was identified as a potential victim in the federal criminal case against Defendant Weiss.¹⁵

¹⁵ See Exhibit A.

79. After receiving notice from the federal government that read: “If you are receiving this notification, it means that information of yours was found in possession of the defendant,”¹⁶ Jane Doe felt violated, deeply disturbed, humiliated, embarrassed, and extremely emotionally distressed; and is experiencing physical manifestations of the stress and anxiety caused by this egregious violation of her privacy, symptoms that are further exacerbated by the fact that Jane Doe still does not have a full and complete understanding of the data breach and cyber voyeurism perpetrated by Defendant Weiss.

80. This cyber voyeurism invaded Plaintiff’s privacy and has devastated her personally and emotionally, as her highly sensitive private information was stolen by an alleged predator under circumstances that were entirely preventable by Defendant Simmons and Defendant Keffer.

81. Upon information and belief, the United States Department of Justice is in the process of notifying thousands of potential victims that their privacy was breached.

82. As a direct result of the negligence, recklessness, and misconduct of the Defendants, Jane Doe and those similarly situated have incurred substantial monetary and emotional damages exceeding \$5,000,000, exclusive of costs, interest, and fees.

F. Keffer and Simmons Failed to Properly Protect Plaintiff’s and Class Members’ PII and PHI

83. Defendants Keffer and Simmons did not use reasonable security procedures and practices, including leaving data unencrypted, appropriate to the nature of the sensitive PII and PHI it was maintaining for Plaintiff and Class Members, causing the breach of PII and PHI for 150,000 students and former students, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for approximately 3,330 students and former students.

¹⁶ *Id.*

84. The FTC takes action when companies make promises to safeguard personal information and then fail to live up to those promises, including by promulgating numerous guides which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

85. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.¹⁷ The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.¹⁸

86. The FTC further recommends that companies not maintain PII and PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

87. Defendants Keffer and Simmons failed to properly implement these basic data security practices explained and set forth by the FTC.

¹⁷ FEDERAL TRADE COMMISSION, *Protecting Personal Information: A Guide for Business*, Oct. 2016, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

¹⁸ *Id.*

88. Defendants Keffer’s and Simmons’s failure to employ reasonable and appropriate measures to protect against unauthorized access to PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

89. A systematic, years-long breach such as the ones Defendants Keffer and Simmons experienced is also considered a breach under the HIPAA Rules because there is unauthorized access to PHI that is not permitted under HIPAA.

90. A breach under the HIPAA Rules is defined as, “the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI.” 45 C.F.R. 164.40.

91. Data breaches are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

The presence of ransomware (or any malware) on a covered entity’s or business associate’s computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. 45 C.F.R.164.308(a)(6).¹⁹

92. Defendants Keffer’s and Simmons’s data breach was the foreseeable consequence of a combination of deficiencies that demonstrate Defendants Keffer and Simmons failed to comply with safeguards mandated by HIPAA.

¹⁹ U.S. DEPT OF HEALTH AND HUM. SERVS., *FACT SHEET: Ransomware and HIPPA*, July 11, 2016, at 4, <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>.

G. Defendants Simmons and Keffer Failed to Comply with Industry Standards

93. Defendants Keffer and Simmons did not utilize industry standards, like encryption, appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the breach of PII and PHI for approximately 150,000 students and former students, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for 3,330 students and former students.

94. As explained by the FBI, “[p]revention is the most effective defense against cyberattacks] and it is critical to take precautions for protection.”²⁰

95. To prevent and detect data breaches, including the breach here that resulted in theft of PII and PHI and cyber voyeurism, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of cyberattacks and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

²⁰ FEDERAL BUREAU OF INVESTIGATION, *How to Protect Your Networks from RANSOMWARE*, at 3, <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Dec. 20, 2024).

- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common cyberware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.²¹

96. To prevent and detect cyberattacks, including the cyberattack that resulted in the data breaches and cyber sexual assaults, Defendants Keffer and Simmons could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure Internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management

²¹ *Id.* at 3-4.

- Perform regular audit; remove privileged credentials

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].²²

97. As described above, experts studying cyber security routinely identify medical facilities as being particularly vulnerable to cyberattacks because of the value of the private information they collect and maintain.

98. Several best practices have been identified that at a minimum should be implemented by institutions such as Defendants Keffer and Simmons, including, but not limited to, the following: educating all employees on security; strong passwords; multi-layer security,

²² MICROSOFT, *Human-Operated Ransomware Attacks: A Preventable Disaster*, Mar. 5, 2020, <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>.

including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

99. Other standard cybersecurity best practices include installing appropriate malware detection software; monitoring and limiting access to network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

100. Given that Defendants Keffer and Simmons were storing the private information of 150,000 individuals combined, Defendants Keffer and Simmons could and should have implemented all of the above measures to prevent cyberattacks, along with two- or multi-factor authentication as discussed earlier in this Complaint.

101. The occurrence, scope, and duration of the breach and cyber voyeurism indicates that Defendants Keffer and Simmons failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the theft of approximately 150,000 students' and former students' PII and PHI, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for 3,330 students and former students.

H. Defendants Keffer and Simmons Failed to Properly Protect PII and PHI

102. Defendants Keffer and Simmons breached their obligations to Jane Doe and Class Members and were otherwise grossly negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches, cyber-attacks, and hacking incidents;
- b. Failing to adequately protect students' private information;
- c. Failing to properly monitor its own computer networks for existing or prior intrusions;
- d. Failing to test and assess the adequacy of its data security system;
- e. Failing to develop adequate training programs related to the proper handling of emails and email security best practices;
- f. Failing to adequately fund and allocate resources for the necessary design, operation, maintenance, and updating required to meet industry standards for data protection;
- g. Failing to require a data security system to ensure the confidentiality and integrity of electronic PHI its network created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- h. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access to only those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);
- i. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);
- j. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);
- k. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. § 164.306(a)(2);
- l. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);
- m. Failing to ensure that it was compliant with HIPAA security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(4);
- n. Failing to train all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its

workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

- o. Failing to ensure that the electronic PHI it maintained is unusable, unreadable, or indecipherable to unauthorized individuals, as Defendants had not encrypted the electronic PHI as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.” (45 C.F.R. § 164.304 definition of encryption);
- p. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;
- q. Failing to adhere to industry standards for cybersecurity.

103. As the result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendants Keffer and Simmons negligently and unlawfully failed to safeguard Plaintiff’s and Class Members’ private, sensitive information.

104. Defendant Simmons was also grossly negligent in its failure to oversee the data security practices of third-party vendor—Keffer—in which it entrusted the sensitive private information of its students and former students.

105. Accordingly, as outlined below, Plaintiff and Class Members have already been severely harmed by this egregious violation of their privacy by Defendant Weiss.

CLASS ALLEGATIONS

106. Plaintiff files this lawsuit both individually and as representative of all others similarly situated pursuant to Fed. R. Civ. P. 23 on behalf of the following Class: All students whose personal data, images, information, social media, or videos were accessed by Weiss without authorization (“Class Members”).

107. In addition, Plaintiff believes a subclass may be appropriate for all class members who receive notice from the United States Department of Justice as to the likely violation of their

privacy and rights by Weiss. Therefore, Plaintiff pleads a subclass as follows: All students whose personal data, images, information, social media, or videos were accessed by Weiss without authorization and who received a notice letter from the United States Department of Justice as to Weiss (“DOJ Letter Sub-Class”).

108. Excluded from the Class are: (a) Defendants and any entity or division in which Defendants have a controlling interest, and their legal representatives, officers, directors, assigns, and successors; (b) the Judge to whom this case is assigned and the Judge’s staff; and (c) the attorneys representing any parties to this Class Action.

109. Plaintiff reserves the right to modify or amend the definition of the proposed class and/or sub-classes before the Court determines whether certification is appropriate.

A. Numerosity – Fed. R. Civ. P. 23(a)(1)

110. Law enforcement officials have disclosed that the number of victims is significant and exceeds one thousand satisfying the numerosity requirement. Although the exact number of Class Members is uncertain at this time and it will certainly be ascertained through appropriate discovery, the number is great enough such that joinder is impracticable.

111. The members of the Class are so numerous and geographically dispersed that individual joinder of all members is impracticable.

112. Similarly, Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, Internet postings, and/or published notice.

113. Class Members are readily identifiable from information and records in the possession of the federal and state authorities, Simmons, and Keffer.

114. Electronic records maintained by Simmons and Keffer can confirm the identification of Class Members.

B. Commonality and Predominance – Fed. R. Civ. P. 23(a)(2) and 23(b)(3)

115. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and the other Class Members. Similar or identical violations, practices, and injuries are involved, and the burden of proof to establish violations of those rights involve uniform, objective questions of fact and law, both for Plaintiff and for Defendants.

116. The common questions of fact and law existing as to all Class Members predominate over questions affecting only individual class members. The evidence required to advance Plaintiff’s and Class Members’ claims are the same, common to all; as is true of the evidence Defendants will likely rely upon in defense of this action. Thus, the elements of commonality and predominance are both met.

117. For example, establishing the facts of how, where, who, when, and through what means the invasions of Plaintiff’s and other Class Members occurred are identical.

118. Defendants’ actions, inactions, negligence, and recklessness apply commonly to Plaintiff and Class Members.

119. The theft of images and invasions by Weiss and the improper conduct of accessing private information through unsecure systems without permission is common to all Class Members and has caused injury to the Plaintiff and Class Members in common manners.

120. The First Circuit has held that “[a]s long as a sufficient constellation of common issues binds class members together,” notwithstanding the existence of some individualized issues, a class may still be certified under Rule 23(b)(3). *Waste Management Holdings, Inc. v. Mowbray*,

208 F.3d 288, 296 (1st Cir. 2000). Liability will be tested under the same standard, equally applicable for all class members, making certification appropriate under Rule 23(b)(3).

121. The majority of legal and factual issues of the Plaintiff and the Class Members predominate over any individual questions, including:

- (a) Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members private information;
- (b) Whether Defendants Keefer and Simmons failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the hacking incident and cyber sexual assault;
- (c) Whether Defendants Keefer and Simmons's data security systems prior to and during the data breach and cyber voyeurism complied with applicable data security laws and regulations;
- (d) Whether Defendants Keefer's and Simmons's data security systems prior to and during the data breach and cyber voyeurism were consistent with industry standards;
- (e) Whether Defendants Keefer and Simmons owed a duty to Plaintiff and Class Members to safeguard their private information;
- (f) Whether Defendants Keefer and Simmons breached their duty to Plaintiff and Class Members to safeguard their private information;
- (g) Whether Defendant Simmons was grossly negligent and/or negligent in its oversight of Defendant Keefer;
- (h) Whether Defendant Simmons or Keefer knew or should have known that their data security systems and monitoring processes were deficient;
- (i) Whether Defendants Keefer and Simmons owed a duty to provide Plaintiff and Class Members timely notice of the data breach and cyber voyeurism, and whether Defendants Keefer and Simmons breached that duty to provide timely notice;
- (j) Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;
- (k) Whether Defendants' conduct was negligent or grossly negligent;
- (l) Whether Defendants' conduct was per se negligent;

- (m) Whether Defendants' conduct violated federal laws;
- (n) Whether Defendants' conduct violated state laws;
- (o) Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or punitive damages; and
- (p) Other common questions of fact and law relative to this case that remain to be discovered.

122. Resolving the claims of these Class Members in a single action will provide benefit to all parties and the Court by preserving resources, avoiding potentially inconsistent results, and providing a fair and efficient manner to adjudicate the claims.

123. Predominance does not require Plaintiff to prove an absence of individualized damage questions. *In re Suffolk Univ. COVID Refund Litig.*, No. 20-10985-WGY, 2022 U.S. Dist. LEXIS 185297, at *5-6 (D. Mass. Oct. 11, 2022) (finding that "the need for individualized damage decisions does not ordinarily defeat predominance where there are still disputed common issues as to liability.") (citing *Tardiff v. Knox Cty.*, 365 F.3d 1, 6 (2004)).

C. Typicality – Fed. R. Civ. P. 23(a)(3)

124. Plaintiff's claims are typical of those of other Class Members because all had their private information compromised as a result of the breach and cyber voyeurism and Defendants' malfeasance.

125. Plaintiff's claims are typical of the Class Members because they are highly similar and the same and related in timing, circumstance, and harm suffered. To be sure, there are no defenses available to Defendants that are unique to individual Plaintiffs. The injury and causes of actions are common to the Class as all arising from the same statutory and privacy interests.

126. In *Halliburton Co. v. Erica P. John Fund, Inc.*, 573 U.S. 258, 276 (2014) the Supreme Court concluded that so long as plaintiffs could show that their evidence is capable of proving the key elements to plaintiffs’ claim on a class-wide basis, the fact that the defendants would have the opportunity at trial to rebut that presumption as to some of the plaintiffs did not raise individualized questions sufficient to defeat predominance. “That the defendant might attempt to pick off the occasional class member here or there through individualized rebuttal does not cause individual questions to predominate.” *Id.*

127. Certification of Plaintiff’s claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

128. The need to conduct additional post certification stage discovery, such as further file review or class member surveys, to eliminate uninjured persons after trial, does not act as a bar to certification. *Astrazeneca AB v. UFCW (In re Nexium Antitrust Litig.)*, 777 F.3d 9, 19 (1st Cir. 2015). “At the class certification stage, the court must be satisfied that, prior to judgment, it will be possible to establish a mechanism for distinguishing the injured from the uninjured class members. The court may proceed with certification so long as this mechanism will be ‘administratively feasible,’ and protective of defendants’ Seventh Amendment and due process rights. *Id.*; see also American Law Institute, Principles of the Law: Aggregate Litigation, §§ 2.02(a)(3), 2.07(d) cmt. j (2009) (indicating that the court should exercise discretion to authorize aggregate treatment only if it would “not compromise the fairness of procedures for resolving any remaining issues presented by such claims” and that “due process in aggregation . . . extend[s] to persons opposing the aggregate group litigating related claims on an aggregate basis.”). By placing

the validation of injury step at the end of the class trial process, no injured class members are left out, and at the same time, Defendants are not at risk for paying any uninjured class members.

D. Adequacy of Representation – Fed. R. Civ. P. 23(a)(4)

129. Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that she has no interests that are in conflict with those of the Class Members. In addition, she has retained counsel competent and experienced in complex class action litigation, and she will prosecute this action vigorously. The Class’s interests will be fairly and adequately protected by Plaintiff and her counsel.

E. Superiority of Class Treatment – Fed. R. Civ. P. 23(b)(3)

130. The class action is superior to any other available procedures for the fair and efficient adjudication of these claims, and no unusual difficulties are likely to be encountered in the management of this class action.

131. The superiority analysis required to certify a class looks at pertinent factors in assessing superiority, such as “the class members’ interests in individually controlling the prosecution or defense of separate actions” and “the likely difficulties in managing a class action.” *Barrett v. H&R Block, Inc.*, No. 08-10157-RWZ, 2011 U.S. Dist. LEXIS 30713, at *25 (D. Mass. Mar. 25, 2011) (citing Fed. R. Civ. P. 23(b)(3)). Superiority exists where “there is a real question whether the putative class members could sensibly litigate on their own for these amounts of damages, especially with the prospect of expert testimony required.” *Gintis v. Bouchard Transp. Co., Inc.*, 596 F.3d 64, 68 (1st Cir. 2010).

132. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable.

133. It would be an unnecessary burden upon the court system to require these individual Class Members to institute separate actions. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

134. Pursuing this matter as a class action is superior to individual actions because:

- (a) Separate actions by Class Members could lead to inconsistent or varying adjudications that would confront Defendants with potentially incompatible standards of conduct;
- (b) Many victims will not come forward without a certified class;
- (c) Final equitable relief will be appropriate with respect to the entire Class as a whole for monitoring, protection, therapy and other equitable forms of relief that may be provided;
- (d) This action is manageable as a class action and would be impractical to adjudicate any other way;
- (e) Absent the class action, individual Class Members may not know if their privacy was invaded; where such images are currently being stored, or are accessible by others; and their injuries are likely to go unaddressed and unremedied; and,
- (f) Individual Class members may not have the ability or incentive to pursue individual legal action on their own.

F. Particular Issues – Fed. R. Civ. P. 23(c)(4)

135. In the event unforeseen issues preclude class certification under Fed. R. Civ. P. 23(b)(3), the case is still appropriate for class certification under Fed. R. Civ. P. 23(c)(4), as to the particular issues of liability.

136. Defendants have acted or refused to act on grounds generally applicable to Plaintiff and the other members of the Class, thereby making declaratory relief, as described below, with respect to the Class as a whole.

COUNT I
VIOLATIONS OF THE COMPUTER FRAUD AND ABUSE ACT – 18 U.S.C. § 1030
(DEFENDANT WEISS)

137. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

138. Weiss violated the Computer Fraud and Abuse Act by unlawfully accessing Plaintiff's private information without authorization.

139. Weiss' actions constituted a violation of the Act because by entering Plaintiff's social media, email, and/or cloud storage accounts, and extracting sensitive private information of students, he "intentionally access[ed] a computer without authorization." 18 U.S.C. § 1030(a)(2)(C).

140. Weiss's actions were deliberate because he knew he was unauthorized and proceeded nevertheless.

141. Under 18 U.S.C. § 1030(g), Plaintiffs may recover damages in this civil action from Weiss along with injunctive relief or other equitable relief.

142. Given the willful violations committed by Weiss, resulting in significant damage, harm, humiliation, and distress to Plaintiffs and other Class Members, Plaintiffs should be awarded all appropriate damages in this matter.

COUNT II
VIOLATIONS OF THE STORED COMMUNICATIONS ACT – U.S.C. § 2701
(DEFENDANTS WEISS, KEFFER, AND SIMMONS)

143. Plaintiffs restate and incorporate the allegations set forth above as if fully set forth herein.

144. Plaintiffs allege that Defendants Weiss, Keffer, and Simmons violated the Stored Communications Act.

145. The Stored Communications Act, 18 U.S.C. § 2701 et seq., prohibits the unauthorized access of web-based cloud storage, email, and social media accounts such as those at issue and other accounts hosted by Defendants Simmons and Keffer that contain personal, private, and intimate information and communications about and relating to Plaintiffs and others situated similarly to Plaintiffs.

146. Specifically, under 18 U.S.C. § 2701(a), it is unlawful for any person to: (1) intentionally access without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceed an authorization to access that facility; and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system.

147. Under 18 U.S.C. § 2702, it is unlawful for a person or entity providing an electronic communication service to the public to knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service or to divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of a subscriber or customer of such service, solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

148. Plaintiffs' electronic information and communications were in electronic storage and clearly fall within the scope of the statute.

149. Defendant Weiss was not authorized to access or divulge the content of Plaintiffs' private communications by for any purpose.

150. The information, messages, files, and media were accessed by Weiss without authorization.

151. Weiss's access without authorization was deliberate.

152. There is no manner in which Plaintiff's and class member's private information, messages, files, and media could have been obtained without unauthorized access and would not have been obtained without unauthorized access had Defendants Keffer and Simmons not knowingly divulged or permitted access to such information, through Defendants' systems and/or Keffer's ATS application, despite knowing that the information would not be protected.

153. Under Section 2707 of the Stored Communications Act, individuals may bring a civil action for the violation of this statute.

154. This law imposes strict liability on violators.

155. The statute provides that a person aggrieved by a violation of the act may seek appropriate relief including equitable and declaratory relief, actual damages or damages no less than \$1,000 punitive damages, and reasonable attorney's fee[s] and other litigation costs reasonably incurred according to 18 U.S.C. § 2707(b)-(c).

156. Defendants' access to and divulging of Plaintiffs' private, personal, and intimate information, messages, files, and media constituted a violation of 18 U.S.C. §§ 2701 and 2702.

157. Defendants Keffer, Simmons, and Weiss knew they did not have authority to access and divulge Plaintiffs' private, personal, and intimate information, messages, files, and media but did so anyway.

158. Defendants' knowing or intentional conduct led to multiple violations of the Stored Communications Act.

159. As a result of these violations, Plaintiffs have incurred significant monetary and nonmonetary damages as a result of these violations of the Stored Communications Act, and Plaintiffs seek appropriate compensation for their damages.

160. Under the statute, Plaintiffs should be granted the greater of (1) the sum of their actual damages suffered and any profits made by Simmons and Weiss as a result of the violations or (2) \$1,000 per violation of the Stored Communications Act.

161. Given these violations were deliberate, the Court should assess punitive damages against Defendants as well.

162. Plaintiffs should also be granted reasonable attorney fees and costs.

COUNT III
VIOLATIONS OF TITLE IX – 20 U.S.C. § 1681(A)
(DEFENDANT SIMMONS)

163. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

164. Title IX mandates that “No person in the United States shall on the basis of sex, be ... subject to discrimination under any education program or activity receiving Federal financial assistance ...”

165. Each Plaintiff and Class Member is a “person” under the Title IX statutory language.

166. Weiss specifically targeted women in his unwanted invasions of privacy and his misconduct is discrimination on the basis of sex.

167. Defendant Simmons receives federal financial support for its educational programs and is therefore subject to the provisions of Title IX of the Education Act of 1972, 20 U.S.C. § 1681(a), *et seq.*

168. Defendant Simmons, under Title IX, is obligated to investigate allegations of sexual harassment.

169. Defendant Simmons was aware of the sensitive nature of the private and personal information of Plaintiffs to which Weiss was able to access given his role.

170. Defendant Simmons acted with deliberate indifference to sexual harassment by:

- a. Failing to protect Plaintiffs and others as required by Title IX;
- b. Neglecting to adequately investigate and address the complaints regarding the deeply sensitive information Plaintiffs provided;
- c. Failing to institute corrective measures to prevent Weiss from sexually harassing other students; and
- d. Failing to adequately investigate the other multiple acts of deliberate indifference.

171. Simmons and its Trustees acted with deliberate indifference as their lack of response to the sexual harassment was clearly unreasonable in light of the known circumstances.

172. Defendant Simmons' failure to promptly and appropriately protect, investigate, and remedy and respond to the sexual harassment of women has effectively denied them equal educational opportunities at the University, including access to medical care and sports training.

173. At the time the Plaintiff and Class Members received some medical training services from Simmons, they did not know Simmons and Keffer failed to adequately consider their safety including in their engagement, hiring, training, and supervision of Weiss.

174. As a result of Defendant Simmons' deliberate indifference, Plaintiff and Class Members have suffered loss of educational opportunities and/or benefits.

175. Plaintiff and Class Members have and incurred, and will continue to incur, attorney's fees and costs of litigation.

176. At the time of Defendants' misconduct and wrongful actions and inactions, Plaintiff and Class Members were unaware, and or with reasonable diligence could not have been aware, of Defendants' institutional failings with respect to their responsibilities under Title IX.

177. Defendant Simmons maintained a policy and/or practice of deliberate indifference to protection of female student athletes.

178. Defendants' policy and/or practice of deliberate indifference to protection against the invasion of privacy for female athletes created a increased risk of sexual harassment.

179. Despite being able to prevent these privacy violations and acts of harassment, Defendants failed to do so.

180. Because of Defendant Simmons's policy and/or practice of deliberate indifference, Plaintiff and Class Members had their privacy invaded and were sexually harassed by Weiss.

181. Plaintiff and Class Members should be awarded all such forms of damages in this case for Defendant Simmons's conduct that caused great damage, humiliation, and embarrassment to Plaintiffs and the Class.

COUNT IV
INVASION OF PRIVACY INTRUSION UPON SECLUSION

182. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

183. Plaintiff's and Class Members' personal social media files, videos, and other images were each in electronic storage and were intended to be kept private.

184. Weiss unlawfully accessed this information.

185. His actions were not authorized.

186. This information would not have been obtained absent the negligence and misconduct of Simmons and Keffer.

187. Plaintiff and Class Members never granted permission to such access.

188. Plaintiff and Class Members feel embarrassed, ashamed, humiliated, and distressed that their private information has been accessed by strangers and third parties.

189. Plaintiff's and Class Members' social media data, images, and other media are private information.

190. Plaintiff and Class Members had the right to expect all this information would remain private.

191. The methods Weiss used to access such information was objectively unreasonable.

192. As a result of Weiss' actions, Plaintiff and Class Members have incurred significant damages as a result of Defendants' actions and request the appropriate damages.

COUNT V
NEGLIGENCE and GROSS NEGLIGENCE

193. Plaintiff restates and incorporates the allegations set forth above as if fully set forth herein.

194. Plaintiff's and Class Members' personal and private information, data, and media was in electronic storage and expected to remain private.

195. That private and personal information, data, and media was accessed by Weiss unlawfully.

196. Weiss' actions were not lawful.

197. The information, data, and media could not have been accessed but for the Non-Individual Defendants' lack of monitoring and supervision of Weiss.

198. Plaintiff and Class Members did not authorize the access to such information, data, and media.

199. Plaintiff and Class Members are embarrassed, ashamed, humiliated, and mortified that their private information has been accessed by total strangers and third parties.

200. Plaintiff's and Class Members' had a right to keep such information, data, and media private.

201. Plaintiff and Class Members entrusted Defendant Simmons and its Trustees to ensure methods were undertaken to secure, safeguard, and protect against unauthorized access to their private information.

202. Keffer was entrusted to keep Plaintiff's and Class Members' private information private.

203. Upon information and belief, Simmons and Keffer admitted that Plaintiff and Class Members expected each of them to take reasonable measures to maintain the privacy of their private information.

204. Defendant Simmons breached their duties to Plaintiff and Class Members by failing to consider, implement, or follow a policy to oversee how or whether Keffer conducted its operations in a manner that would have in any manner monitored, supervised, and ensured that

engagement, retention and/or employment of Weiss would not result in a breach of the privacy Plaintiff and Class Members entrusted to Defendant Simmons.

205. Plaintiff and Class Members entrusted Defendant Simmons and its Trustees to take measures to ensure Weiss did not gain unauthorized access to their private information, data, and media.

206. Defendant Simmons failed in this duty by failing to take any action to prevent the harm caused to Plaintiff and Class Members as alleged in this Complaint, including but not limited to the inaction of failing to implement a policy to monitor, supervise, and oversee Weiss, or ensure more than one person is verifying that such sensitive and personal and private information is kept confidential.

207. Defendant Simmons were supposed to, but failed, to establish a policy, including to monitor personnel, including but not limited to Weiss, so that students on the campus are protected from their privacy being invaded.

208. Defendant Simmons failed to provide security to Plaintiffs and to other student athletes to be able to be treated by athletic professionals who do not invade their privacy.

209. Keffer recklessly failed to ensure media and information of and pertaining to student athletes including but not limited to Plaintiff and Class Members was safely provided and stored even after Plaintiff and others similar to them entrusted Keffer to do so.

210. Defendant Simmons had an obligation to support Plaintiff and Class Members, and to develop the campus, its operations including student services, and admissions, and financial aid, among others, in a way that at least considered having and executing security measures to protect the personal, private, and intimate images and information of the Plaintiff and others similar to them.

211. Defendant Simmons breached those duties when they failed to implement security measures to protect the private and personal data, information, and media of Plaintiffs was not unlawfully accessed.

212. Defendant Simmons had a duty but failed to learn, enact, or implement any security measures to protect the personal, private, and intimate images and information of the Plaintiff and Class Members.

213. Given the sensitive nature of the Plaintiffs' private information, Simmons and Keffer knew of and, as detailed herein, breached their heightened duties to safeguard and protect Plaintiff's and Class Members' privacy by failing to implement security measures, and that recklessness exposed Plaintiff, the Class, and their private and personal data, information, and media.

214. Defendant Simmons' failures and omissions in these respects was so reckless that it shows a substantial lack of concern for injuries to Plaintiff and the Class.

215. Defendant Simmons's failures and omissions in these respects was so reckless that it shows a substantial lack of concern for injuries to Plaintiff and the Class.

216. Keffer's failures and omissions in these respects was so reckless that it shows a substantial lack of concern for injuries to Plaintiff and the Class.

217. Plaintiff and Class Members have incurred significant damages as a result of Defendants' actions, and should be awarded damages accordingly.

RELIEF

WHEREFORE, Plaintiff prays this Court grant the following relief:

- a. Enter a judgment encompassing the relief requested above, plus significant compensatory damages exceeding \$5,000,000.00 together with costs, interest and attorney fees, against Defendants, and such other relief to which they are entitled;

- b. An order certifying the proposed Class and Subclasses; designating Plaintiff as the named representative of the respective Class Members; and appointing her counsel as Class Counsel;
- c. All such equitable relief as the Court deems proper and just, including but not limited to, declaratory relief;
- d. Award Plaintiff costs, attorney fees as well as interest from the date of Judgment until paid; and
- e. Grant such further relief as is agreeable to equity and good conscience.

JURY DEMAND

For all triable issues, a jury is hereby demanded.

Dated: April 28, 2025

Respectfully Submitted,

The Plaintiff,
Jane Doe
By her attorneys,

/s/ Paula S. Bliss

Paula S. Bliss (BBO# 652361)
Kimberly A. Dougherty (BBO# 658014)
Justice Law Collaborative, LLC
210 Washington Street
North Easton, MA 02356
Telephone: (508) 230-2700
Facsimile: (285) 278-0287
paula@justicelc.com
kim@justicelc.com

Megan Bonanni (P52079)*
Kevin M. Carlson (P67704)*
Beth M. Rivers (P33614)
Danielle Y. Canepa (P82237)
Pitt McGehee Palmer Bonanni & Rivers
117 W. Fourth Street, Suite 200

Royal Oak, MI 48067
(248) 398-9800
mbonnani@pittlawpc.com
kcarlson@pittlawpc.com
brivers@pittlawpc.com
dcanepa@pittlawpc.com

Lisa M. Esser (P70628)*
Richard L. Groffsky (P32992)*
Jason J. Thompson (P47184)*
Matthew G. Curtis (P37999)*
SOMMERS SCHWARTZ, P.C.
One Towne Square, 17th Floor
Southfield, MI 48076
(248) 355-0300
LEsser@sommerspc.com
rgroffsky@sommerspc.com
JThompson@sommerspc.com
MCurtis@sommerspc.com

Ryan Clarkson*
Bryan Thompson*
Timothy Giordano
Yana Hart
Clarkson Law Firm
22525 Pacific Coast Highway
Malibu, CA 90265
(213) 471-2599
rclarkson@clarksonlawfirm.com
bthompson@clarksonlawfirm.com
tgiordano@clarksonlawfirm.com
yhart@clarksonlawfirm.com

**Pro hac vice forthcoming*

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

Jane Doe

(b) County of Residence of First Listed Plaintiff Plymouth County
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)
Paula S. Bliss, Justice Law Collaborative
210 Washington St., North Easton, MA 02356
(508) 230-2700

DEFENDANTSSimmons University, The Trustees of Simmons University,
Matthew Weiss, and Keffer Development Services, LLC

County of Residence of First Listed Defendant Suffolk County
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF
THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff ☒ 3 Federal Question (U.S. Government Not a Party)
- ☐ 2 U.S. Government Defendant ☐ 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- | | PTF | DEF | | PTF | DEF |
|---|----------------------------|----------------------------|---|----------------------------|----------------------------|
| Citizen of This State | <input type="checkbox"/> 1 | <input type="checkbox"/> 1 | Incorporated or Principal Place of Business In This State | <input type="checkbox"/> 4 | <input type="checkbox"/> 4 |
| Citizen of Another State | <input type="checkbox"/> 2 | <input type="checkbox"/> 2 | Incorporated and Principal Place of Business In Another State | <input type="checkbox"/> 5 | <input type="checkbox"/> 5 |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3 | <input type="checkbox"/> 3 | Foreign Nation | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 |

IV. NATURE OF SUIT (Place an "X" in One Box Only)Click here for: [Nature of Suit Code Descriptions.](#)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES	
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice	PERSONAL INJURY <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act IMMIGRATION <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 PROPERTY RIGHTS <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 835 Patent - Abbreviated New Drug Application <input type="checkbox"/> 840 Trademark <input type="checkbox"/> 880 Defend Trade Secrets Act of 2016 SOCIAL SECURITY <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit (15 USC 1681 or 1692) <input type="checkbox"/> 485 Telephone Consumer Protection Act <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input checked="" type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
REAL PROPERTY <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	CIVIL RIGHTS <input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education	PRISONER PETITIONS Habeas Corpus: <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty Other: <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN (Place an "X" in One Box Only)

- ☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District (specify) ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
18 U.S.C. § 1030, 18 U.S.C. § 2701, 15 U.S.C. § 6851, 20 U.S.C. § 1681(A), 42 U.S.C. § 1983

Brief description of cause:

Unauthorized cyber invasion and violation of private electronically stored personal information of college students.

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND \$

>\$5,000,000.00

CHECK YES only if demanded in complaint:

JURY DEMAND:☒ Yes ☐ No**VIII. RELATED CASE(S) IF ANY**

(See instructions):

JUDGE

DOCKET NUMBER

DATE

SIGNATURE OF ATTORNEY OF RECORD

4/28/2025

/s/ Paula S. Bliss

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS1. Title of case (name of first party on each side only) Jane Doe v. Simmons University

2. Category in which the case belongs based upon the numbered nature of suit code listed on the civil cover sheet. (See local rule 40.1(a)(1)).

☐

I. 160, 400, 410, 441, 535, 830*, 835*, 850, 880, 891, 893, R.23, REGARDLESS OF NATURE OF SUIT.

☐

II. 110, 130, 190, 196, 370, 375, 376, 440, 442, 443, 445, 446, 448, 470, 751, 820*, 840*, 895, 896, 899.

☒

III. 120, 140, 150, 151, 152, 153, 195, 210, 220, 230, 240, 245, 290, 310, 315, 320, 330, 340, 345, 350, 355, 360, 362, 365, 367, 368, 371, 380, 385, 422, 423, 430, 450, 460, 462, 463, 465, 480, 485, 490, 510, 530, 540, 550, 555, 560, 625, 690, 710, 720, 740, 790, 791, 861-865, 870, 871, 890, 950.

*Also complete AO 120 or AO 121. for patent, trademark or copyright cases.

3. Title and number, if any, of related cases. (See local rule 40.1(g)). If more than one prior related case has been filed in this district please indicate the title and number of the first filed case in this court.

4. Has a prior action between the same parties and based on the same claim ever been filed in this court?

YES

☐

NO

☒

5. Does the complaint in this case question the constitutionality of an act of congress affecting the public interest? (See 28 USC §2403)

YES

☐

NO

☒

If so, is the U.S.A. or an officer, agent or employee of the U.S. a party?

YES

☐

NO

☒

6. Is this case required to be heard and determined by a district court of three judges pursuant to title 28 USC §2284?

YES

☐

NO

☒

7. Do all of the parties in this action, excluding governmental agencies of the United States and the Commonwealth of Massachusetts ("governmental agencies"), residing in Massachusetts reside in the same division? - (See Local Rule 40.1(d)).

YES

☒

NO

☐

A. If yes, in which division do all of the non-governmental parties reside?

Eastern Division

☒

Central Division

☐

Western Division

☐

B. If no, in which division do the majority of the plaintiffs or the only parties, excluding governmental agencies, residing in Massachusetts reside?

Eastern Division

☐

Central Division

☐

Western Division

☐

8. If filing a Notice of Removal - are there any motions pending in the state court requiring the attention of this Court? (If yes, submit a separate sheet identifying the motions)

YES

☐

NO

☒

(PLEASE TYPE OR PRINT)

ATTORNEY'S NAME Paula S. BlissADDRESS 210 Washington St., North Easton, MA 02356TELEPHONE NO. (508) 230-2700

Exhibit A

From: U.S. Department of Justice - VNS <fedemail@vns.usdoj.gov>
Sent: Monday, March 31, 2025 6:13 PM
To: [REDACTED]
Subject: U.S. Department of Justice - VNS - Investigative Case 288A-DE-3728795 - Court Case 25-CR-20165

DO NOT REPLY TO THIS EMAIL.



March 31, 2025

U.S. Department of Justice
Eastern District of Michigan
Suite 2001
211 W. Fort St.
Detroit, MI 48226-3211
Phone: 1-844-527-5299
Email: USAEO.MCAP@usdoj.gov

[REDACTED]

Re: United States v. Defendant(s) Matthew Weiss
Case Number 2023R00208 and Court Docket Number 25-CR-20165

Dear [REDACTED]:

The enclosed information is provided by the United States Department of Justice Victim Notification System (VNS). As a victim witness professional, my role is to assist you with information and services during the prosecution of this case. I am contacting you because you were identified by law enforcement as a victim or potential victim during the investigation

of the above criminal case.

As a result of the numerous inquiries regarding the United States v. Matthew Weiss matter, below please find information as to the most frequently asked questions (FAQ).

- **What are the charges?**

The defendant was charged with 10 counts of Unauthorized Access (18 U.S.C. section 1030) and 14 counts of Aggravated Identity theft (18 U.S.C. section 1028(A)(a)(1)). The indictment can be found by going here: <https://www.justice.gov/usao-edmi/us-v-matthew-weiss> .

- **How was I personally affected?**

The investigation has identified more than 3,300 victims of Unauthorized Account Access. These accounts include social media, cloud storage, and/or email accounts. If you were notified as a victim, you were identified among this group of individuals. The investigation has also identified more than 150,000 individuals whose personally identifiable information (PII) was obtained through unauthorized access to a third-party database. Additional PII was found, the exact source of which is not known. The quantity and type of information found for each individual varies. Notifications were not issued solely based on the defendant's possession of PII. If you were notified as a victim, it is because evidence was found indicating unauthorized access into at least one of your online accounts.

- **Which accounts of mine were accessed?**

Accounts accessed include social media, cloud storage and email accounts. The FBI cannot definitively say the total number of accounts accessed for each individual. If you were notified as a victim, it is because evidence was found indicating unauthorized access into at least one of your online accounts. This evidence includes, but is not limited to, the defendant's documentation of access into victim accounts.

- **Do we know what types of photos obtained?**

The defendant had an assortment of photos; majority of them were private and sensitive in nature. Some also included photos of identity documents such as passports and driver's license.

- **Did the defendant have any sensitive or private photos or videos of all the victims?**

NO! *The amount of data, existence of photos/video, and level of documentation varies for every individual. Additionally, we are not able to*

confirm the identity of all individuals in photos and videos found in the investigation.

Victims notified in this case were notified because evidence was found indicating unauthorized access into at least one of their online accounts. In some cases, victims were identified through sensitive photos and/or videos found in the investigation. This is not the case for every victim in this investigation. The FBI cannot confirm which information, photos, or videos were viewed by the defendant.

- **Were my photos/videos shared or posted online?**

We have no indication the compromised information or content was further shared or distributed by the defendant. This investigation is ongoing and involves thousands of victims. We are not able to confirm the identity of all individuals in photos and videos found in this investigation.

- **How was my personally identifying information taken?**

There are multiple potential sources for the personally identifying information exposed in this investigation. We cannot attribute the exact source of all information exposed by the defendant in this case. One known source was the unauthorized access by the defendant of a third-party database. The investigation has identified more than 150,000 individuals whose personally identifying information was obtained through this access. Additional personally identifying information was found, the exact source of which is not known.

- **Am I in danger?**

*There are many victims in this case, across a wide geographic area. We have no reason to believe you are in physical danger related to this investigation. If you have any concerns for your immediate physical safety, contact **9-1-1**.*

If you have further questions, please reach out and contact the *Mega Victim Case Assistance Program (MCAP)* toll free 1(844)527-5299 (Monday through Friday from 8:30 am to 5:30 pm Eastern), or send an email to USAEQ.MCAP@usdoj.gov. Please include your Victim Identification Number (**VIN**), found in the closing paragraph of the first letter, when contacting MCAP via phone or email. If you are having technical difficulties with the Victim Notification System, please contact the VNS Help Desk at the numbers found in the closing of this notification. You can also check for notifications and updates at: <https://www.justice.gov/usao-edmi/case/us-v-matthew-weiss> .

A status hearing is scheduled before Judge Nancy Edmunds for April 15, 2025, 10:30 AM at Courtroom 811, 231 W Lafayette Blvd, Detroit, MI 48226 for defendant(s) Matthew Weiss. The purpose of this hearing is to determine if there are issues that the Court needs to address and to schedule any necessary future court dates.

Because of the Court's schedule, hearing dates could change on very short notice. If you plan on attending, you may want to call the VNS Call Center or check the website to confirm the date and time. Please note, there is a 24-hour delay in information transfer to the website.

Through the Victim Notification System (VNS) we will continue to provide you with updated scheduling and event information as the case proceeds through the criminal justice system. You may obtain current information about this case on the VNS website at <https://www.notify.usdoj.gov> or from the VNS Call Center at 1-866-DOJ-4YOU (1-866-365-4968) (TDD/TTY: 1-866-228-4619) (International: 1-502-213-2767). In addition, you may use the Call Center or Internet to update your contact information and/or change your decision about participation in the notification program.

VIN information removed from forwarded message.

Remember, VNS is an automated system and cannot answer questions. If you have other questions which involve this matter, please contact this office at the number listed above.

Sincerely,

Alexandra Wyatt
Victim Services Coordinator

If you do not want to receive email notifications from the Victim Notification System (VNS) please log into the VNS Web site at <https://www.notify.usdoj.gov>, select "My Information", remove your email address and click the "update" button. If you remove your email address, you will continue to receive letters from VNS except in those case which have large numbers of victims. To change your email address, select "My Information", provide a new address and click the "update" button.

If you do not want to receive any notifications in your case, select "Stop Receiving Notifications" and follow the instructions on the screen.

If you believe you have received this email in error, please contact the office listed at top of the email message.

Please note, if this is the first notification you have received from VNS you will need to wait 4-8 hours from receipt of this email before you can login to the VNS Internet site (<https://www.notify.usdoj.gov>). In addition, it will also be 4-8 hours before any documents which may have been uploaded to VNS as part of this notification are available under the "Downloads/Links" section on the Web page.

Please call the Victim Notification System (VNS) Help Desk at phone number 1-866-625-1631 for assistance and questions.

Disclaimer

The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

This email has been scanned for viruses and malware, and may have been automatically archived by Mimecast, a leader in email security and cyber resilience. Mimecast integrates email defenses with brand protection, security awareness training, web security, compliance and other essential capabilities. Mimecast helps protect large and small organizations from malicious activity, human error and technology failure; and to lead the movement toward building a more resilient world. To find out more, visit our website.

Exhibit B

Athletic Trainer System



EMR Software

**Empowering Athletic Trainers and Staff for More
Efficient Documentation & Coordinated Environment**

- ★ **HIPAA & FERPA compliant** ★ **FedRAMP certified data center**
- ★ **100% US owned & operated company** ★ **All data stored in the U.S.**



Athletic Trainer System
24 Village Park Drive
Grove City, PA 16127

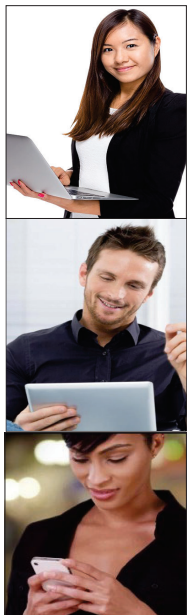
1-888-328-2577
info@athletictrainersystem.com
www.athletictrainersystem.com





Trusted by:

- ✓ High schools, colleges, industrial, hospitals & clinics in 49 states
- ✓ 25,000+ Users.
- ✓ 2,000,000+ Million Athletes.



ATS Modules

- ATS Desktop
- ATS Staff Phone
- ATS Staff Portal
- ATS Athlete Portal & Phone
- ATS Kiosk
- ATS Quick Med Check
- ATS Family Communications Center



**CUSTOMER
SERVICE**
IS NOT A DEPARTMENT.
It **IS AN
ATTITUDE.**



Customer support is one of ATS' highest priorities

- We want to know if you are experiencing issues with your program because we want to fix it.
- If you have any suggestions on a new feature, or something we can add to enhance ATS, do not hesitate to call or email.





Key features

We work with and support Athletic Trainers at every level. This includes the high school, college, hospital, and industrial settings. Our extensive reach reflects our platform's reliability and adaptability to various athletic and healthcare environments.

1. Customer Service and Support Excellence:

- **Searchable help center** where users can quickly find answers to their questions about using the system (e.g., how to register, how to log injuries) from over 400+ docs & videos.
- **Video tutorials** on commonly used features such as setting up profiles, entering daily info, and managing injury reports.
- **Live chat support** provides real-time assistance when the user can't find the documentation they need.

2. Online Athlete Forms & Reports:

- Mobile-friendly athlete forms for injury reporting, consent, and health tracking.
- Automatic report generation for coaches or healthcare partners with detailed injury status, recovery stages, and alerts.

3. Daily Info Entry:

- Daily entry/update of athlete information and treatments.
- Information includes notes, modalities, rehabs, limitations, medication services, referrals, equipment checkout.
- Athletes list may be filtered by teams, daily login and more.

4. "Copy" Functionality:

- **"Copy last entry"** button for athletes or staff to quickly duplicate previous day's data or notes (e.g., same treatment plan, rehab exercises, or progress update).
- Ability to **copy information** from past injury reports or evaluations to reduce redundant data entry.
- **Multi-entry copy** feature, allowing staff to copy information across multiple athletes at once (e.g., same strength training exercises for the entire team).

5. "Quick" Functionality:

- **Quick-entry forms** for common tasks, such as updating injury status, logging a treatment session, or creating practice plans.
- **Quick note** feature that allows users to leave **short updates** (e.g., "Athlete cleared for light practice").
- **Pre-set quick buttons** for frequently used actions.

6. Athlete Multi-Function Update:

- **Bulk update tool** where staff can edit multiple athlete profiles at once (e.g., updating the year in school or adding a limitation notice to an entire team).
- **Global updates** to apply injury status changes.
- Quick access to **multi-function dashboards** for medical staff to see at a glance which athletes need attention or follow-up.

7. Robust Reporting Tools

- With 700+ reports covering injuries, staff performance, travel details, and more.
- ATS provides insights that help streamline operations and improve outcomes.
- Data Miner query tool.
- ROI and crosstab analytics reports.





Highlighted Features

Full circle communication

- Group email/text messages for non-staff.
- Secure message to athlete, contacts & staff.
- Appointment reminders.
- Injury Journal to show history.
- Group notices for staff.
- Batch reports for coaches/staff.
- Batch notes for emergency contacts.

View Your Data Multiple Ways

- 700+ reports for all areas.
- Data miner.
- Injury Analytics.
- Admin dashboard.
- Screens on your laptop, PC & phone.

Concussions

To better protect our clients and student athletes, our concussion module stands above others in the industry offering 6 customizable evaluation templates built around the SCAT, BESS, SAC, VOMS & more.

Nightly Sync with other software

ATS now has a process that allows our clients to sync information from other software systems to their ATS database.

Coaches are able to...

- ✓ Securely access athlete information (emergency contacts, insurance, paperwork) from their phones
- ✓ Communicate with athletes or parents securely
- ✓ Can receive automated report(s)
- ✓ Can receive timely updates on injuries
- ✓ Easily communicate with medical staff
- ✓ See paperwork & cleared-to-play status
- ✓ See injury, practice & game status

Data Miner, ROI

- In addition to the 700+ reports, the "Data Miner" allows you to select and export data to Microsoft Excel.
- Our ROI reports show productivity and validation for staff and equipment.



**Video
Overview**



**Request
a demo**



Contact Us



Website



Facebook



LinkedIn



YouTube



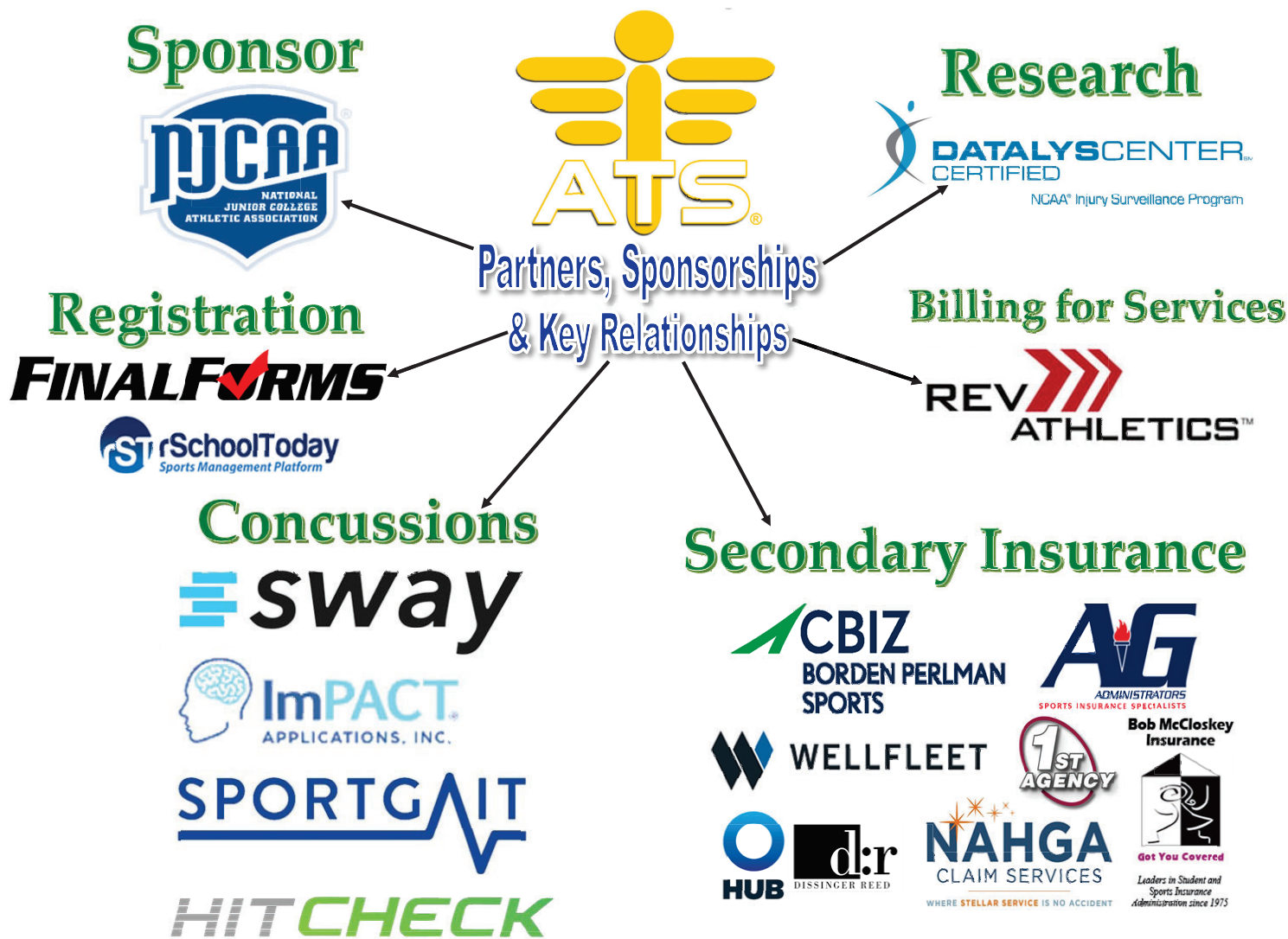


Exhibit C

Company History



Since 1994, Keffer Development Services—also known as The Athletic Trainer System (ATS)—has been at the forefront of custom software design and development.

What began in the basement of our family home has grown significantly over the years. In 1996, we relocated to downtown Grove City, PA, and in 2005, we built our own facility just outside of town.

In 2008, ATS welcomed its first client, and since then, we have been fortunate to collaborate with over 600 clients across 48 states and internationally. Our diverse clientele includes high schools, colleges of all levels, outreach programs, and industrial settings.

We are renowned for our exceptional customer support and our openness to client feedback and suggestions. Our mission is to address the evolving needs of the sports medicine community, including athletic trainers, medical professionals, athletes, students, coaches, administrators, and parents.

Our Business Philosophy

We strongly believe in professional ethics and “old school” customer service:

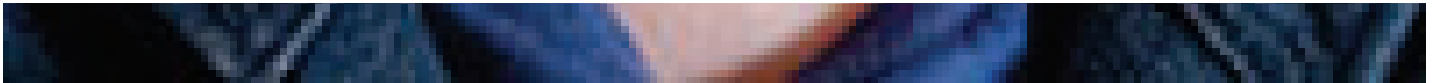
- * When you call during our business hours you will likely talk to one of us.
- * If you email us for help we usually get back to you quickly; no longer than the next business day.
- * Our online help library has 100s of help docs and 100s of help videos. The library is searchable for users.
- * Our ATS staff will help you configure your ATS software to meet your needs.
- * We have the technology, experience, and relationships to help you accomplish your goals.

The bottom line...

We want our users to be confident about referring us to friends and colleagues.

Meet the Team





Ashley, ATC

Sales & Support



Joe, ATC

Sales & Support



Gail

Research & Sales



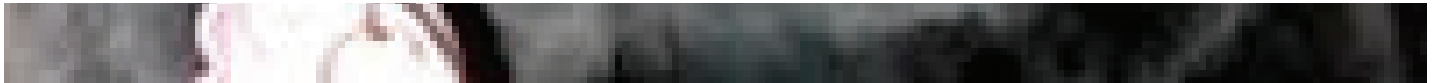
Dana
Office Manager



Rhett

Founder/CEO





Maggie

Office Security

Exhibit D

0:00 / 1:20

The ATS electronic medical records system is by far the best advancement to US
Fencing Sports Medicine!
Jeremy Summers, Team Doctor

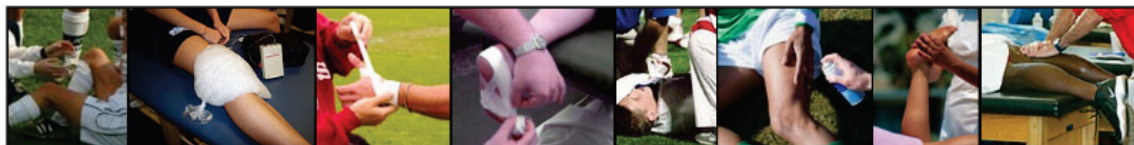
Absolutely the best software out there for all of your athletic training needs. This
software just keeps getting better with the updates that are made available. Well worth
the price and I'm very happy that I chose ATS for my athletic training software.
Jeff Schirf, AT, Bridgeton HS

Customer service is outstanding!!
Christine Scuderi, Head AT, SUNY Canton

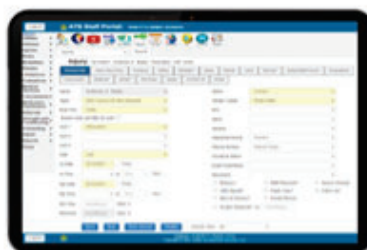
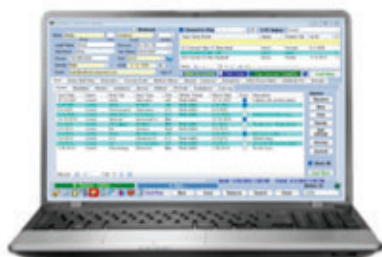
[View all testimonials... \(Testimonials.aspx\)](#)

THE Athletic Trainer System An Electronic Health Record System...

- ✓ Designed with Athletic Trainers for ALL Medical Professionals
- ✓ Serving 6500+ schools, clinics & other organizations.
- ✓ 27,000+ Users and 2+ Million Athletes.



Access Real-Time Data 24x7x365



For Medical Professionals working with...

Athletes



Students

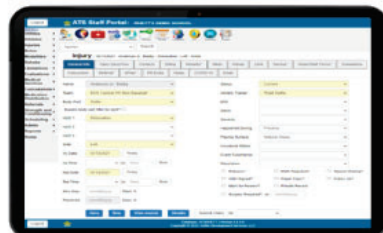
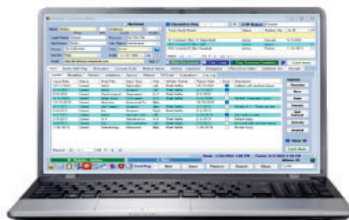


Employees



Concussion Evaluations

Included with ATS...no additional cost

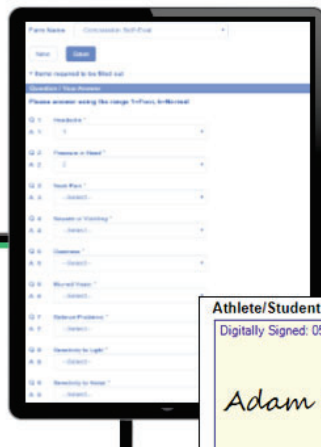
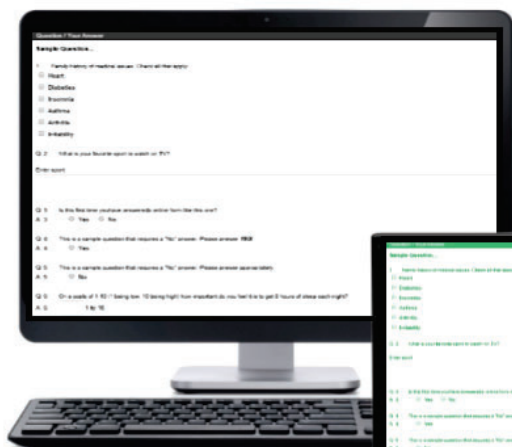


On your phone, laptop or tablet

AND import info from our partners

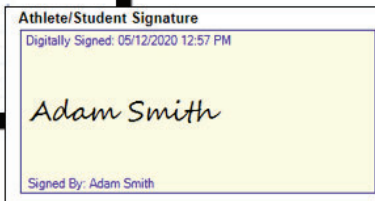


Online Registration



- Custom Forms
- Demographics
- Insurance
- Contacts
- Immunizations
- Scheduling

Forms Library



Digital Signatures

Student Registration Partners

FINAL* *FORMS



Secondary Insurance Claim Submission

Through the ATS System claims may be submitted quickly and easily. Claim formats & processes have been approved with our partners shown here.



Bob McCloskey Insurance
BMI BENEFITS - FULL TPA SERVICES



Billing for Athletic Training Services...

- Rehabs & Modalities are entered by your medical staff
- Claims are created using our claim utility
- Claims are submitted for payment by our billing partner
- An eFile, HCFA-style, copy of the claim information sent is saved in the injury and athlete area(s).



Our billing partner:
Rev-Athletics
 mpb@rev-athletics.com
 rev-athletics.com



Customer Service & Support

**CUSTOMER
 SERVICE**
IS NOT A DEPARTMENT.
**IS AN
 ATTITUDE.**

**At ATS we are
 known for our
 availability to
 help our users
 and respond
 to requests for
 system enhancements.
 Help is available by phone,
 email & 300+ docs & videos**



Exhibit E



The Athletic Trainer System®

FAQ

I'd like to try **ATS** before purchasing. How do I do that?

We have a fully functional demo database with a good number of athletes and teams already set up. You will have access to all the modules available with ATS so you can explore the functionality. We also do web demos via GoTo meeting.

Call, email or click [demo request](#) to request a demo log in, schedule a meeting or to discuss the options.

Where is our data stored?

Keffer Development hosts all databases in our SSAE-16, SOC II and FedRamp certified data center. This means your data never is stored outside the United States, and will be available anywhere you have internet or cellular access. We have additional information you can share with your IT department if needed.

- **If our data is stored on your server who owns it?**

Each ATS Client owns their data. Information security is a high priority in our company. We do not share your data or sell the information. If our relationship ends we will gladly send you a copy of your data upon request within 30 days of cancellation.

Is ATS HIPAA and FERPA compliant?

On top of our Data Center being FedRamp Certified, ATS is also HIPAA and FERPA compliant. We utilize a company called Compliance Helper to ensure we maintain HIPAA and FERPA compliance. Please review the [Compliance Helper page](#) on our website for more information.

How much does ATS cost?

ATS has a wide variety of packages available to suit your programs needs.

More details can be found on our [current pricing](#).

- **Is there is an added cost for additional users or computer/workstation installs?**

ATS does not limit the amount of downloads of the program. ATS is licensed by user ranges, not the downloads. Please refer to the pricing guide for information on the groups for billing.

- **Are there any added costs for additional functionality like concussion evaluations or kiosk stations?**

The standard ATS has no additional costs. We do have additional options for larger eFile sizes, "encrypted at rest" data and our ATS Data Exchange functionality.

What kind of customer support/service does ATS provide?

With initial purchase of ATS, 2(two) hours of training are included, to help setup and customize the system. Also there is training for the staff to help with the transition. Beyond that, standard support is available by phone, email, web meetings, and a library of help docs and videos.

We invite you to talk with your fellow ATCs. We have worked hard to build and maintain a reputation for customer service and support. We are happy to provide references.

May I see a list of your current clients?

References available upon request. To make that request, please use the link here to [Contact Us](#).

Call: 1-888-328-2577 email: info@athletictrainersystem.com

Visit: www.athletictrainersystem.com





The Athletic Trainer System®

FAQ

What kind of devices can I use to run ATS?

ATS was designed to work with a variety of devices. Contact us for more details.


Do you have an "App" for phones or tablets?

Our "apps" are browser-based, and do not install on phones/tablets. From a security standpoint most "apps" on phones/tablets store PHI info on the device, which is a big issue should the device be lost or stolen.

Does ATS support 2-factor Authentication?

Yes, we have our own 2-factor authentication that can be enabled for staff and/or athletes/guardians.

Can I create/export a report to other formats?

All reports in the ATS system may be exported to a variety of formats, including, PDF, Encrypted PDF, MS-Word, MS-Excel along with other options. 

ATS also can work with your email client to send encrypted attachments. These features can be restricted based on user specific security.

What business partners does ATS have?

- Secondary Insurance Carriers, and ability to submit electronic claims. See the [Secondary Partners Doc.](#)
- [REV Athletics](#), is our 3rd party billing Partner.
- [rSchool Today](#) serves as a partner for demographics and registration.
- [SWAY Medical](#), serves as our partner to seamlessly load their concussion reports into ATS
- [Datalys](#) and the NCAA Injury Surveillance Program, allow you to submit injury information via ATS directly to Datalys.

Does ATS communicate to hospital based EMR systems?

Yes, as an additional component to the standard options. The additional feature allows the AT Staff the ability to send athlete or injury information to any hospital/clinic based EMR system. This process is dependent on them being a part of the National Data Exchange.

Cost associated with sending information:

There is a 1-time set up fee of \$150 to establish the connection. The yearly fee is \$100 per billable user.

Call: 1-888-328-2577 email: info@athletictrainersystem.com
Visit: www.athletictrainersystem.com





The Athletic Trainer System®

FAQ

Can athletes/guardians register and/or access ATS remotely?

Yes. The ATS Athlete Portal and Family Communication Center provides this ability through secure connections. This includes demographic information, emergency contact information and online forms that may be electronically signed. Athletes/Parents may also access information from the ATS Athlete Smartphone.

More information is available in [our brochure](#).

Can I have multiple teams? multiple sports? multiple schools?

Yes. Your ATS database may have as many teams, sports and schools as are needed. In addition you are able to give users security access based on the teams you define. e.g. restrict users to seeing athletes on only the specific teams you choose.

Can an athlete belong to more than one team?

Yes. Athletes may belong to as many teams as needed.

How can I share with guardians/parents my interactions with their Athlete?

We have an Activity Journal/Injury Tree, that you have the option to share with guardians/parents. This is visible from the athletes portal and shows the interaction with the athlete.

If I have an athlete transfer how do I send their information with them?

ATS has a report that can be ran and sent with the athlete that contains all of their information. If they are transferring to or from a school that uses ATS already, you can use the Athlete Send feature to send their information directly to the new schools ATS database.

What ways does ATS allow me to communicate with my staff, parents/guardians, athletes, coaching staff or my Physicians?

ATS has many ways to aid with communication. Please refer to our [Communication Doc](#) for further explanation of the capabilities.

How does ATS increase productivity and timely documentation?

We have an Injury Updates Needed list. It will display your injured athletes in one of three indicators Red, Yellow, Green. You will be able to custom set the days of last data entry for each level. Indicator levels are based on date of last documentation (note modality rehab). For example: if someone hasn't had interaction for example 8 days, they will be listed in red.

Do I have to manually enter all of my Athletes in to ATS?

ATS has several ways to populate your athletes. In addition to manually entering athletes, you can have the Athlete register through the Athlete Portal or utilize our Standard Import utility. You can also have your IT department set up a Nightly Sync process with us. We also have a partnership with rSchool Today.

Do you have an "athlete check-in" or something like this?

Our Athlete Kiosk allows customized ability have athlete check-in, log modalities or rehabs if desired, report injuries and more. Further information is available [here](#).

Call: 1-888-328-2577 email: info@athletictrainersystem.com

Visit: www.athletictrainersystem.com





The Athletic Trainer System®

FAQ

Can ATS be accessed by staff from remote locations?

Your staff may access their ATS data securely through the Staff Portal, the Staff Smartphone or the Staff Quick Med Check.

What scheduling functionality does ATS offer?

Comprehensive scheduling features, including:

- View staff schedules
- Schedule athlete appointments
- Allow athletes to book appointments with staff
- Athletes can view their schedule via Athlete Phone or Athlete Portal
- Automated appointment reminders can be sent to staff, athletes and coaches

How can ATS save us time and money?

There are many options that allow quick and efficient data entry, from the Daily Information Entry Screen, to being able to do an injury evaluation from the sideline. We have a 3rd party vendor who is helping bill for Athletic Training services to recoup money spent. As well as an ROI report that allows you the ability to see what would have been spent on referring athletes to Physical Therapy.

How do I customize ATS to be inclusive?

ATS has many ways to customize data collection. Including gender options, personal pronouns, nickname, preferred names, COVID vaccination status and many others.

Does ATS allow me to look at injury trends or statistics?

ATS come equipped with two possibilities:

- Each ATS database comes with the Injury Analytics Reporting feature. This allows you to see trends and number of injuries within your own database.
- We also have the [ATS Sports Medicine Research](#), which allows you to see de-identified injury information across our client base. For more info [Contact Us](#).

Do you have a library of pre-loaded forms I can utilize?

We have a large library (approx. 100) of created documents you can copy from. Examples:

- Medical History/PPE
- Permission/Consent to Treat
- NCAA Recommended Mental Health Forms
- Concussion, Sick Cell, and SCA awareness forms.
- Along with many others

Why do you have an advisory council?

In addition to the input from the ATs on staff, we value opinions, thoughts and ideas from all of our clients. We realize that including thoughts from other medical professionals with a variety of day-to-day experiences can add specifics on what they need from an EMR system. For that reason we do not try to anticipate the needs of these professionals but rely on a representative group to advise us on what would help make their jobs easier.

Call: 1-888-328-2577 email: info@athletictrainersystem.com

Visit: www.athletictrainersystem.com



Exhibit F

Keffer Development Services, LLC Privacy Policy

Last updated: July 2, 2024

Keffer Development Services, LLC. (“KDS”) is committed to maintaining the security and privacy of

personal information collected through this website, www.atsusers.com (the “Website”), the KDS electronic health record (the “EMR”) and the various KDS portals (the “Athlete Portals”). This Privacy Policy discloses KDS’ information collection and dissemination practices in connection with the Website, the EMR and the Athlete Portals and applies solely to the information that we collect through those means. This Privacy Policy does not address personal information that you provide to us in other contexts (e.g., through another relationship not expressly described in this Privacy Policy).

The Electronic Health Record

KDS provides the web-based Clinical EMR to customers who enter into an Athletic Trainer System Agreement (“Customers”), who then authorize Clinical EMR users, including athletic trainers, coaches, physicians, physician assistants, nurse practitioners and non-physician staff members (“Authorized Users”). Customers and Authorized Users are responsible for determining uses and disclosures of patient medical information maintained in the Clinical EMR, in accordance with their legal and professional responsibilities as health care professionals and state and federal medical privacy laws, including the federal Health Insurance Portability and Accountability Act (“HIPAA”). To the extent that KDS receives or maintains patient medical information in the course of providing the Clinical EMR, that information is secured, used and disclosed only in accordance with KDS’ legal obligations as a “business associate” under HIPAA.

The ATS Athlete Portal & ATS Athlete Smartphone

KDS Customers may choose to make the ATS Athlete Portal and/or ATS Athlete Smartphone available to patients to enable certain interactions between the Customer, Authorized Users and patients, including scheduling appointments, discussing medical treatment, sending medication prescription-related messages, and enabling patient viewing of a portion of the Clinical EMR. Customers are solely responsible for the content of the patient’s medical record maintained in the Clinical EMR and determining the portion of the Clinical EMR that may be viewed by the patient through the Patient Portal.

KDS may utilize patient medical information on a limited basis as necessary to provide the Patient Portal services, including the following uses and disclosures:

- Unless the patient is self-registering basic demographics including an email address and login/password are required to be stored in the Clinical EMR before an invitation can be sent to the patient to open a Patient Portal account.
- When an online form or similar function is complete by the patient through the ATS Athlete Portal or ATS Athlete Smartphone, a notice may be generated for Authorized Users.

Cookies

Cookies are pieces of information that a website transfers to a user's computer for purposes of storing information about a user's preferences. Cookies in and of themselves do not personally identify users, although they do identify a user's computer. Many websites use cookies as a standard practice to provide useful features when a user visits the website and most web browsers are set up to accept cookies. KDS uses cookies to improve your online experience when visiting the Website. You can set your browser to refuse cookies, but some portions of the Website may not work properly if you refuse cookies. Some of the Website's web pages may use web beacons in conjunction with cookies to compile aggregate statistics about website usage.

Security

KDS understands that storing our data in a secure manner is essential. KDS stores PII, PHI and other data using industry-standard physical, technical and administrative safeguards to secure data against foreseeable risks, such as unauthorized use, access, disclosure, destruction or modification. Please note, however, that while KDS has endeavored to create a secure and reliable website for users, the confidentiality of any communication or material transmitted to/from the Website or via e-mail cannot be guaranteed.

Personal Information Provided by You

Except as described in this Privacy Policy, KDS only collects your personally identifiable information ("PII") and Protected Health Information ("PHI") through this Website when you choose to provide such information, such as when you use the "Contact Us" feature or submit a job application. PII can include your name, date of birth and zip code. KDS uses your PII to address your requests for information, products or services. KDS will not sell, rent, license, or trade your PII with third parties for their own direct marketing use unless we receive your express consent to do so. Unless you give us permission to do so, KDS will not share your PII other than as specified in this Privacy Policy

Disclosures to Third Parties Assisting In Our Operations

KDS may share your PII under confidentiality agreements with other companies that work with, or on behalf of, KDS to provide products and services. These companies, which may include members of KDS' corporate family, may use your PII to assist KDS in its operations. However, these companies do not have any independent right to share this information.

Disclosures Under Special Circumstances

We may provide information about you to respond to subpoenas, court orders, legal process or governmental regulations, or to establish or exercise our legal rights or defend against legal claims. We believe it is necessary to share information in order to investigate, prevent or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, or as otherwise required by law.

Business Transfers

We may share your PII with other business entities, in connection with the sale, assignment, merger or other transfer of all or a portion of KDS' business to such business entity. We will require any such successor business entity to honor the terms of this Privacy Policy.

Changes to this Privacy Policy

We may update Our Privacy Policy from time to time.

Contact Us

If you have any questions about this Privacy Policy, You can contact us:

- By email: security@kefferdevelopment.com